Volume

2

EverFocus

User Manual

NAV IP Access Controller

EFC302
EFC304
EFC306
EFC308

EVERFOCUS ELECTRONICS CORPORATION

EFC302
EFC304
EFC306
EFC308

User Manual

© 2009~2011 EverFocus Electronics Corp

All rights reserved. No part of the contents of this manual may be reproduced or transmitted in any form or by any means without written permission of the EverFocus Electronics Corporation.

Contents

1. Introduction 1
1.1 Features 2
1.2 Overview 3
1.3 Specification 4
1.4 Packing List 6
1.5 Optional Device 6
1.6 Definitions of Terminal Block and LEDs 7
1.6.1 Terminal Block and LEDs on Main Module 7
1.6.2 Terminal Block and LEDs on Alarm Module 8
1.6.3 Terminal Block and LEDs on Door Module 9
2. Installation 11
2.1 Installation Preparation 11
2.1.1 Obtain a Floor Plan 11
2.1.2 Determine the Hardware and Location 12
2.1.3 Determine the Number of Controllers/ Modules According to System Structure 13
2.2 Hardware Installation 13
2.2.1 Mounting the Enclosure (Optional) and Controller 13
2.2.2 Installing and Connecting the Readers 17
2.2.3 Connecting to the Door Lock, Sensor and Open Button 18
2.2.4 Connecting to the Fire Alarm/ Alarm Input 20
2.2.5 Connecting to the Fire Alarm/ Alarm Output 21
2.2.6 Connecting to the Computer through the Network 22
2.2.7 Mounting a Backup Battery in the Enclosure (Optional) 22
3. System Architecture and Connections 23
3.1 Small System for 8 Doors 23
3.2 System for 256 Doors 23
3.3 System for More theN 256 Doors 24
3.4 RS485 Bus Extension 24
4. Starting Up the Controller 26
4.1 Connecting to Power 26
4.2 Restoring the Controller 26
4.3 Before First Use 27
5. Controller Configuration and Operation 28
5.1 General Operation Guideline 28
5.2 Home Screen 28
5.3 Direct Operations from Keypad 29
5.3.1 Enter System Configuration 29
5.3.2 Enter Arm/Disarm Menu 29

5.3.3 Display Firmware Version 29
5.3.4 Display the Number of Installed Modules 30
5.3.5 Display the Current Card and Event Number 30
5.3.6 Display the Controller IP Address 30
5.4 Level One System Configuration Items 30
5.5 System Setting 31
5.5.1 Enter System Setting Menu 31
5.5.2 Set Date Format 31
5.5.3 Set Date 31
5.5.4 Set Time 32
5.5.5 Auto Daylight Saving Time 32
5.5.6 Set System PIN 32
5.5.7 Set Arm PIN 33
5.5.8 Set Language 33
5.5.9 Backlight Setting 33
5.5.10 System Maintanence 33
5.5.11 Erase All Events 35
5.5.12 Load Factory Default 35
5.6 Card Setting 35
5.6.1 Enter Card Setting Menu 35
5.6.2 Add Cards 36
5.6.3 Delete Cards 36
5.6.4 Set Card Properties 37
5.6.5 Show Card Number 40
5.7 Door Setting 40
5.7.1 Enter Door Setting Menu 40
5.7.2 Schedule Switch Setting 40
5.7.3 Door Access Mode 41
5.7.4 Open Time Setting 42
5.7.5 Over TimeSetting 42
5.8 Reader Setting 43
5.8.1 Enter Reader Setting Menu 43
5.8.2 System Reader Setting 43
5.8.3 Keypad Setting 43
5.8.4 Reader to Door Allocation 44
5.8.5 Reader Backlight Setting 44
5.8.6 Set Reader LED or LCD format 44
5.8.7 Set Card Format 45
5.9 Alarm Setting 45
5.9.1 Components for Alarm 46
5.9.2 Alarm Configuration Basics 46
5.9.3 Enter Alarm Setting Menu 46
5.9.4 Alarm Setting Menu Structure 47
5.9.5 Alarm Input Setting 47
5.9.6 ALarm Event Setting 51
5.10 Network Setting 56
5.10.1 DHCP Setting 56
5.10.2 Set IP Address 57
5.11 Address Setting 57
5.12 Arm/Disarm 58
5.12.1 Arm the Systemusing the Controller Keypad 58

5.12.2 Disarm the Systemusing the Controller Keypad 58
5.12.3 Reset Alarm 59
5.12.4 Arm/Disarm the Systemusing aKeypad Reader 59
5.12.5 Arm/Disarm the Systemusing aLCDReader 60
5.13 Use Reader as Keypad 60
6. Software Introduction 62
6.1 Main Feature 62
6.2 Hightlight Performance Overview 62
6.3 Baseon TCP/IP Access Conttrol System Architecture 63
7. Start to Use 64
7.1 Quick Start 64
7.1.1 Add and Configure Controller 64
Set Access Rule 64
7.1.3 A Varietyof WaystoAdd Cards 66
7.1.4 Setup Departemnt and Cardholder 67
7.1.5 Configuration and Attendance 67
7.1.6 Real-time Monitoring 68
7.1.7 Export Function 68
7.1.8 Print Function 70
7.2 Login 70
7.3 Familiar with the Browser Page 71
7.3.1 Main Page Introduction 71
7.3.2 Menus 72
7.3.3 Control Pannel 72
7.3.4 Real-time Monitoring 74
7.3.5 System Event Record 74
8. Basic Setting 77
8.1 Change Password 77
8.2 Set User Group and User 78
8.3 User Group 80
8.3.1 Add A Group 80
8.3.2 Edit A Group 80
8.3.3 Delete A Group 80
8.4 User Setting 81
8.4.1 Add A User 81
8.4.2 EditA User 82
8.4.3 Delete A User 82
8.4.4 Export Users 82
8.4.5 Print Users 82
8.4.6 Search Users 83
8.5 Local Server 83
8.6 System Upgrade 84
8.6.1 Upgrade Online 84
8.6.2 Upgrade Local 84
9. Cardholder 85
9.1 Department Setting 85

9.1.1 Add A Department 85
9.1.2 Edit A Department 86
9.1.3 Delete A Department 86
9.2 Cardholder Setting 87
9.2.1 Add ACardholder 87
9.2.2 EditA Cardholder 91
9.2.3 Delete A Cardholder 92
9.2.4 Export CardHolders 92
9.2.5 PrintCardHolders 92
9.2.6 Search CardHolders 92
9.3 ImportCardholders 92
10. Real-time Monitoring 94
10.1 Real-time Event 94
10.1.1 Remote Controller 95
10.1.2 Remote Dvr and View 95
10.2 Edit Electronic Map 95
10.2.1 Add An Electronic Map 95
10.2.2 Edit An Electronic Map 96
10.2.3 Delete An Electronic Map 97
10.3 Report 97
10.3.1 Search Cardholders 97
10.3.2 Export Cardholders 97
10.3.3 Print Cardholders 98
11. Maintenance 99
11.1 Backup 99
11.1.1 Manual Backup 99
11.1.2 Auto Backup 100
11.2 Restore 101
11.2.1 Restore from a FTP Server 101
11.2.2 Restore from Local Computer 101
11.3 PurgeOut-of-date Data 102
12. Controller 103
12.1 Controller Setting 103
12.1.1 Add A Controller 103
12.1.2 Edit A Controller 104
12.1.3 Delete A Controller 105
12.1.4 Refresh 105
12.1.5 Setting 105
12.1.6 Export Controllers 113
12.1.7 Print Controllers 114
12.1.8 Download Data to Controller 114
13. Access Rule 115
13.1 Date Type 115
13.1.1 AddA Date 115
13.1.2 Delete A Date 116
13.2 Group Schedule 116
13.2.1 Add A Group Schedule 117

13.2.2 Delete A Group Schedule 117
13.2.3 Edit A Group Schedule 117
13.2.4 Save As A New Schedule 119
13.3 Access Group 119
13.3.1 Add A Access Group 119
13.3.2 Delete A Access Group 120
13.4 Door Schedule 120
13.4.1 Add A Door Schedule 120
13.4.2 Delete A Door Schedule 121
13.4.3 Edit A Door Schedule 121
13.4.4 Save As A New Schedule 122
13.5 Access Door 122
14. Card 123
14.1 Card Type Setting 123
14.2 Card Setting 124
14.2.1 AddA (Batch) Card 124
14.2.2 EditA (Batch) Card 126
14.2.3 Delete A (Batch) Card 126
14.2.4 Export Cards 126
14.2.5 Print Cards 126
14.2.6 Search Cards 127
14.3 Import Cards 127
15. Report 129
15.1 CardReport 129
15.1.1 Search Cards 129
15.1.2 Export Cards 129
15.1.3 Print Cards 129
15.2 Card-dependent Event 130
15.2.1 Search Events 130
15.2.2 Export Events 130
15.2.3 Print Events 130
15.3 Card-independent Event 130
15.3.1 Search Events 131
15.3.2 Export Events 131
15.3.3 Print Events 131
16. Attendance Basic Setting 132
16.1 Attendance Time 132
16.1.1 Edit Attendance Time 133
16.1.2 Search Attendance Time 133
16.1.3 Export Attendance Time 133
16.1.4 PrintAttendance Time 133
16.2 Week Holiday Setting 134
16.2.1 Edit AWeek Holiday 134
16.2.2 SearchWeek Holidays 134
16.2.3 Export Week Holidays 135
16.2.4 Print Week Holidays 135
16.3 Special Holiday Setting 135

16.3.1 Add A SpecialHoliday 135
16.3.2 EditA SpecialHoliday 136
16.3.3 RemoveA SpecialHoliday 136
16.3.4 SearchSpecialHolidays 136
16.3.5 ExportSpecialHolidays 136
16.3.6 PrintSpecialHolidays 137
17. Attendance Exception 138
17.1 No-Access-Attendance 138
17.1.1 AddA No-Access-Attendance 138
17.1.2 EditA No-Access-Attendance 139
17.1.3 DeleteA No-Access-Attendance 139
17.1.4 SearchNo-Access-Attendance 139
17.1.5 ExportNo-Access-Attendance 140
17.1.6 PrintNo-Access-Attendance 140
17.2 Time-off Enroll 140
17.2.1 AddTime-off Enroll 141
17.2.2 EditTime-off Enroll 141
17.2.3 DeleteTime-off Enroll 142
17.2.4 Search Time-off Enroll 142
17.2.5 ExportTime-off Enroll 143
17.2.6 PrintTime-off Enroll 143
17.3 Overtime Enroll 143
17.3.1 Add Overtime Enroll 143
17.3.2 Edit Overtime Enroll 144
17.3.3 DeleteOvertime Enroll 145
17.3.4 SearchOvertime Enroll 145
17.3.5 ExportOvertime Enroll 145
17.3.6 PrintOvertime Enroll 145

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
    - Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Chapter
1

1. Introduction

The NAV IP access controller is a powerful Linux-based controller with modular design. You can add up to 4 door modules to the NAV controller for expanding the control scale of up to 8 doors / readers. Or you can add one alarm module to the NAV controller to manage up to 10 alarm inputs and 18 alarm outputs.

Moreover, each NAV controller can connect up to 31 EverFocus' Flex series controllers to expand the control scale of up to 256 doors / readers. You can connect to the NAV controller via network to remotely review, monitor all the events on NAV and Flex controllers and configure all 31 Flex series controllers from the same built-in browser-based management software. Furthermore, you can optionally install multiple NAV controllers for a larger scale access control system. By doing so, you will need the enterprise level Navigation software installed as a central server to manage the large access control system.

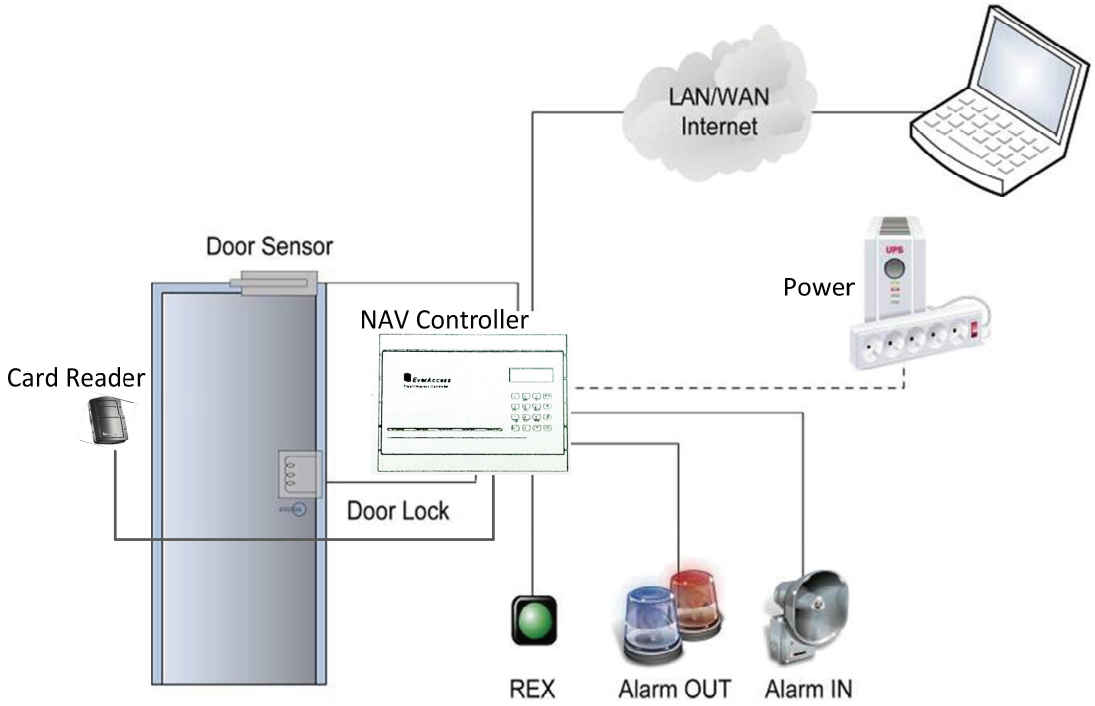


Figure 1-1

The following table lists the models of NAV IP access controllers along with the supported number of doors, readers and alarm inputs / outputs. A description for the supported modules and devices is also provided below.

NAV IP Access Controllers	
Model Name	**Description**
EFC302	• Supports 2 doors, 2 readers • Supports 2 alarm inputs, 4 alarm outputs
EFC304	• Supports 4 doors, 4 readers • Supports 4 alarm inputs, 6 alarm outputs
EFC306	• Supports 6 doors, 6 readers • Supports 6 alarm inputs, 8 alarm outputs
EFC308	• Supports 8 doors, 8 readers • Supports 8 alarm inputs, 10 alarm outputs
Optional Devices / Modules	
Name	**Description**
Door Module	Each NAV controller can add up to 4 door modules. Each door module controls up to 2 readers, 2 relays for door locks, 2 relays for alarm outputs, other door control peripherals, and event signals to the main
Alarm Module	Each NAV controller can add only one alarm module. The alarm module can connect up to 8 alarm inputs and 8 alarm outputs.
Flex Series Controller	Each NAV controller can connect up to 31 Flex series controllers. Each Flex series can connect up to 8 doors and 8 readers.

1.1 Features

- Embedded Linux operating system
- Built-in database engine
- Built-in 512M large-capacity memory
- Modular design for easy expansion of the system, and auto-detection on expansion modules
- Manage up to 31 EverFocus' Flex Series controllers
- Secure access through the Web browser is guaranteed by SSL (Secure Socket Layer)
- Network automatic backup and upgrade
- USB2.0 automatic backup and controller firmware upgrade
- Remote setting, control and management; no software needed to be installed
- Manage up to 100,000 cards and 1,000,000 event records
- Supports 2,048 management groups
- Supports 2,048 access schedule
- Supports 12 kinds of access pattern
- Supports card / group mode to access the door

- Supports 4 x 4 lock level, achieves 4 teams x 4 multi cards access setting on each door
- Each door supports 10 different independent day setting (Sunday to Monday, and 3 kinds of custom day setting). Each day can take 10 time zones with minimum 1 minute duration
- Supports comprehensive access features including interlock, area-based anti passback, multi-card / multi-level access control, panic open, remote door control, system arm / disarm, multiple door verification mode, and first card, etc.
- Multiple languages support: English, Chinese and Russian

1.2 Overview

The diagram below illustrates the controller along with its main components and functions.

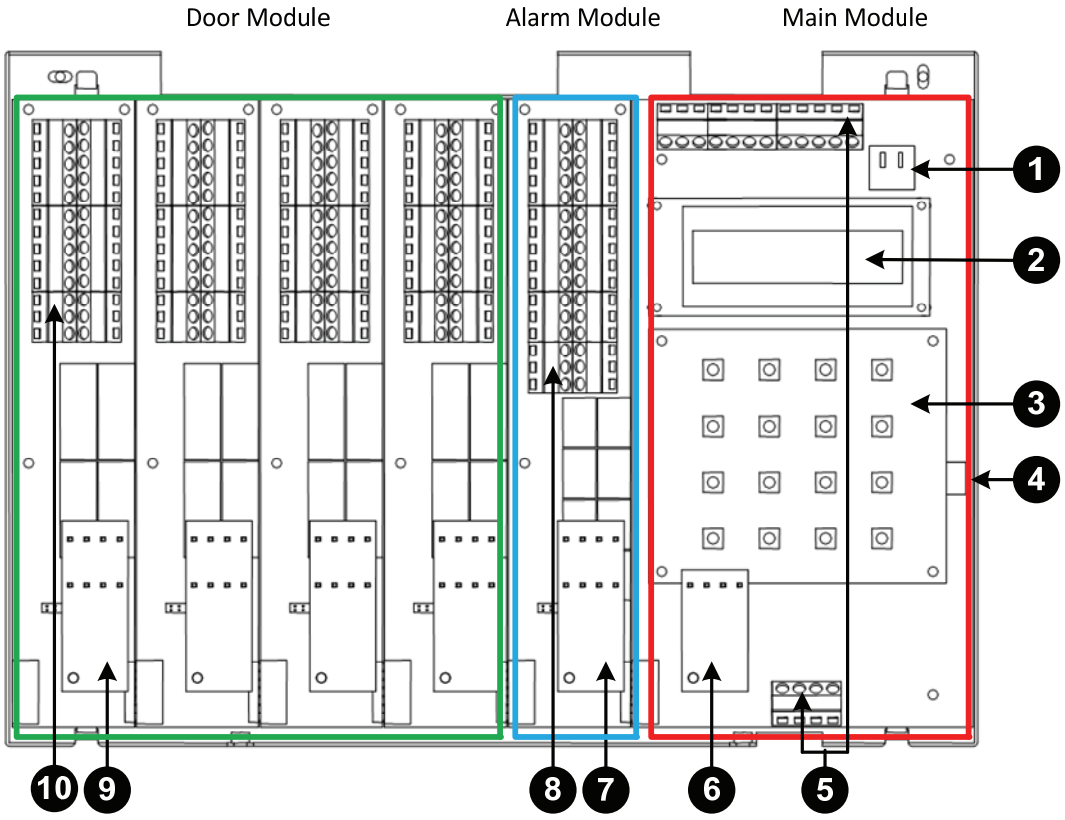


Figure 1-2

Main Module		
The main module controls the fundamental functions of the controller, including the built-in browser-based software, the system management, the power supply, event records, built-in Ethernet port, and communication via RS-485 port, two alarm inputs and two alarm outputs. The main module also controls the door modules and alarm module.		
No.	**Name**	**Description**

1	NetworkPort	Connects to the network.
2	LCD Screen	Displays the current status of the controller and the menu.
3	Keypad	Provides an interface to operate the controller.
4	USB2.0 Port	For database backup / restore and firmware upgrade.
5	Terminal Block	Connects to power, alarm input / output devices, etc. Please refer to *1.6.1 Terminal Block and LEDs on Main Module.*
6	LEDs	Indicates the controller status. Please refer to *1.6.1 Terminal Block and LEDs on Main Module.*

Alarm Module

The alarm module is used to extend the controller's alarm function, adding up to 8 alarm inputs and 8 alarm outputs. Each controller can only add one alarm module.

No.	Name	Description
7	LEDs	Indicates the alarm status. Please refer to *1.6.2 Terminal Block and LEDs on Alarm Module.*
8	Terminal Block	Connects to alarm input / output devices. Please refer to *1.6.2 Terminal Block and LEDs on Alarm Module.*

Door Module

The door module is used to control up to 2 readers, 2 relays for door locks, 2 relays for alarm outputs, other door control peripherals, and event signals to the main module. Each controller can add up to 4 door modules.

No.	Name	Description
9	LEDs	Indicates the door module status. Please refer to *1.6.3 Terminal Block and LEDs on Door Module.*
10	Terminal Block	Connects to door sensors, door locks, request-to-exit devices and alarm outputs. Please refer to *1.6.3 Terminal Block and LEDs on Door Module.*

1.3 Specification

System	
Operating System	Linux embedded
Database	Built-in
Memory	512M
Management Software	Built-in browser-based software, EFS2000, ENS2000

Built-in Software	Supports system management, device configuration, live event list view and map view, CCTV integration
Operation	
Maximum Card Amount	100,000
Maximum Even Records	1,000,000
Supporting Readers	2 (expandable up to 8)
Supporting Door Control	2 (expandable up to 8)
Max. Flex Controllers Connected via RS-485	Up to 31 controllers
Reader Communication Format	Wiegand26 / RS-232
Card / System PIN	8 digits
Alarm PIN	8 digits
Alarm Input	2 (expandable to 10, each alarm input can be set as firmware alarm or regular alarm.)
Alarm Output	2 alarm outputs on main module, 2 alarm outputs on each door module and 8 alarm outputs on alarm
Network Interface	100M adaptive Ethernet interface
Baud Rate	9600 bps
Programmable Duration	Maximum 10 per day with minimum duration of 1 min.
Programmable Date	Sunday to Saturday and 3 customized date types on each individual door.
Access Group	2,048
Access Schedule	2,048
Door Access Verification	12 modes
Other Functions Support	Supports multiple doors interlock, card expiration, anti-passback, backup battery connection, backup battery charger, real-time clock and 4 x 4 lock level (achieves 4 teams x 4 multi cards access setting on
Mechanical	
LCD Display Screen	2 × 9(for Chinese / Russian characters), 2 x 18(for English characters)
Buzzer	Built-in
Keypad	4 x 4 key

General	
Current for Door Control Relay	5A (Max.)
Current for Alarm Relay	2A (Max.)
Power Supply	DC11V ~ 16V (DC 15V when backup battery is
Maximum Current	2A
Dimension (L x W x H)	300 × 216 × 33 mm / 11.8 x 8.5 x 1.3 in

Temperature	14°F~122°F
Humidity	<90%
Weight	1.2 kg / 2.65 lbs

1.4 Packing List

Please check that there is no missing item in the package before installing.

- NAV Controller x 1 (EFC302)
- Supporting Frames (left and right) x 2
- Mounting Template x 1
- 3 x 6 mm screw x 2 (for mounting the controller to the frame)
- User's Manual x 1

Note: Contact the shipper if any items appear to have been damaged in the shipping process. If any items are missing, notify your EverFocus Electronics Corp. Sales Representative or Customer Service Branch. Please also keep the shipping carton for possible future use.

1.5 Optional Device

Optional device can expand your controller's capabilities and versatility. Please contact your dealer for more information.

- EverFocus mental enclosure (EPN-871-B)
- EverFocus USB reader (ERU871)
- EverFocus proximity readers (ERR-871, ERK-871, ERM-871)

1.6 Definitions of Terminal Block and LEDs

1.6.1 Terminal Block and LEDs on Main Module

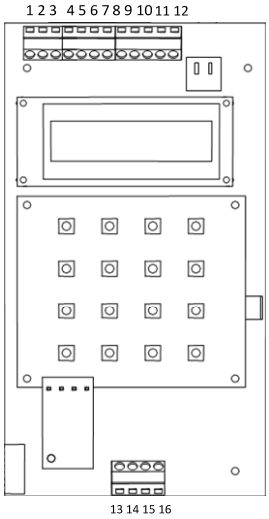


Figure 1-3

Terminal Block Definitions

No	Terminal Name	Function	No.	Terminal Name	Function
1	Alarm In 0	General alarm input 0	10	RS485_A	Signal A of RS-485 bus
2	GND	Alarm input GND	11	COMM_GND	GND of RS-485
3	FireIn	Fire alarm input	12	RS485_B	Signal B of RS-485 bus
4	AUXAlarmOutNo	Normally open pin of auxiliary alarm output	13	Power	Power input
5	AUXAlarmOutCom	Common pin of auxiliary alarm output	14	GND	Power GND
6	AUXAlarmOutNC	Normally close pin of auxiliary alarm output	15	BATT+	Battery positive pin
7	AUXAlarmOutNo	Normally open pin of main alarm output	16	BATT-	Battery negative pin
8	AUXAlarmOutCom	Common pin of main alarm output	17	USB	USB port
9	AUXAlarmOutNC	Normally close pin of main alarm output	18	Ethernet	Ethernet port

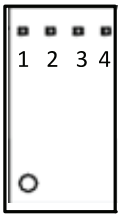


Figure 1-4

LED Definitions

No	Description	No	Description
1	The power is on when the light is on.	3	The data is received when the light is on.
2	The fire alarm is triggered when the light is on.	4	The data is transmitted when the light is on.

1.6.2 Terminal Block and LEDs on Alarm Module

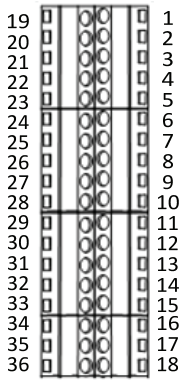


Figure 1-5

No	Terminal Name	Function	No.	Terminal Name	Function
1	Alarm1_In	Alarm signal input 1	19	Alarm5_In	Alarm signal input 5
2	GND	GND	20	GND	GND
3	Alarm2_In	Alarm signal input 2	21	Alarm6_In	Alarm signal input 6
4	Alarm3_In	Alarm signal input 3	22	Alarm7_In	Alarm signal input 7
5	GND	GND	23	GND	GND
6	Alarm4_In	Alarm signal input 4	24	Alarm8_In	Alarm signal input 8
7	Alarm1_NO	Alarm 1 output for NO	25	Alarm5_NO	Alarm 5 output for NO
8	Alarm1_COM	Alarm 1 output in common	26	Alarm5_COM	Alarm 5 output in common
9	Alarm1_NC	Alarm 1 output for NC	27	Alarm5_NC	Alarm 5 output for normally-close
10	Alarm2_ NO	Alarm 2 output for NO	28	Alarm6_ NO	Alarm 6 output for NO
11	Alarm2_ COM	Alarm 2 output in common	29	Alarm6_ COM	Alarm 6 output in common
12	Alarm2_ NC	Alarm 2 output for NC	30	Alarm6_ NC	Alarm 6 output for NC
13	Alarm3_ NO	Alarm 3 output for NO	31	Alarm7_ NO	Alarm 7 output for NO
14	Alarm3_ COM	Alarm 3 output in common	32	Alarm7_ COM	Alarm 7 output in common
15	Alarm3_ NC	Alarm 3 output for NC	33	Alarm7_ NC	Alarm 7 output for NC
16	Alarm4_ NO	Alarm 4 output for NO	34	Alarm8_ NO	Alarm 8 output for NO

17	Alarm4_ COM	Alarm 4 output in common	35	Alarm8_ COM	Alarm 8 output in common
18	Alarm4_ NC	Alarm 4 output for NC	36	Alarm8_ NC	Alarm 8 output for NC

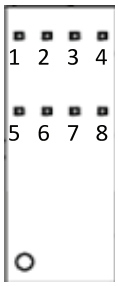


Figure 1-6

LED Definitions

No	Description	No	Description
1	Alarm 1	5	Alarm 5
2	Alarm 2	6	Alarm 6
3	Alarm 3	7	Alarm 7
4	Alarm 4	8	Alarm 8

1.6.3 Terminal Block and LEDs on Door Module

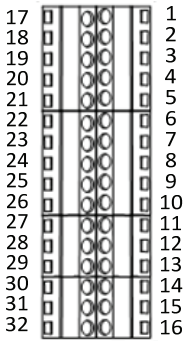


Figure 1-7

No	Terminal Name	Function	No.	Terminal Name	Function
1	Reader1_Data0	Reader 1 Wiegand Data 0	17	Reader2_Data0	Reader 2 Wiegand Data 0
2	Reader1_Data1	Reader 1 Wiegand Data 1	18	Reader2_Data1	Reader 2 Wiegand Data 1
3	Reader1_DC	Power supply for reader 1	19	Reader2_DC	Power supply for Reader
4	Reader1_GND	GND for the Reader 1	20	Reader2_GND	GND for the Reader 2
5	Reader1_Ctrl	Control line for reader 1	21	Reader2_Ctrl	Control line for Reader 2
6	RX_1	Port to TX signal to reader 1	22	RX_2	Port to TX signal to Reader 2
7	TX_1	Port to RX signal from reader 1	23	TX_2	Port to RX signal from Rader 2

8	Door1_ Button	The request-to-exit button for Door 1	24	Door2_ Button	The request-to-exit button for Door 2
9	Door1_GND	GND for terminal 8 & 10	25	Door2_GND	GND for terminal 24 & 26
10	Door1_ Sensor	Door sensor input for Door 1	26	Door2_ Sensor	Door sensor input for Door 2
11	Door1_NO	Normally open pin for door control relay 1	27	Door2_NO	Normally open pin for door control relay 2
12	Door1_COM	Common pin for door control relay 1	28	Door2_COM	Common pin for door control relay 2
13	Door1_NC	Normally close pin for door control relay 1	29	Door2_NC	Normally close pin for door control relay 2
14	Alarm1_NO	Normally open pin for alarm output relay 1	30	Alarm2_NO	Normally open pin for alarm output relay 2
15	Alarm1_COM	Common pin for alarm output relay 1	31	Alarm2_COM	Common pin for alarm output relay 2
16	Alarm1_NC	Normally close pin for alarm output relay 1	32	Alarm2_NC	Normally close pin for alarm output relay 2

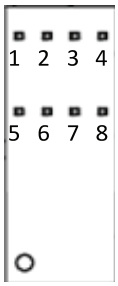


Figure 1-8

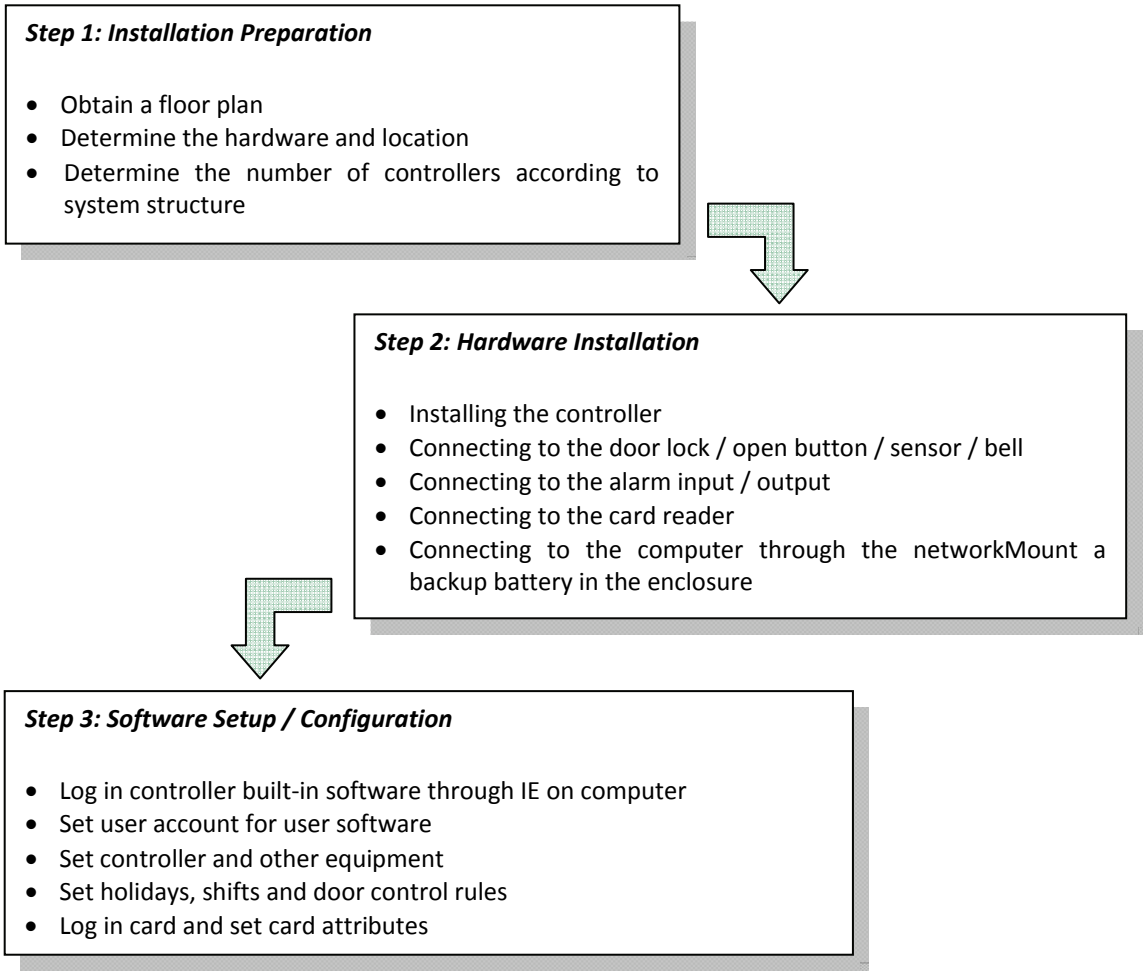
LED Definitions

No	Description	No	Description
1	Indicates the alarm relay #2 is energized.	5	Indicates the alarm relay #1 is energized.
2	Indicates the reader #2 is connected.	6	Indicates the reader #1 is connected.
3	Indicates the door sensor #2 is off (the door's open).	7	Indicates the door sensor #1 is off (the door's open).
4	Indicates the door control relay #2 is energized.	8	Indicates the door control relay #1 is energized.

Chapter 2

2. Installation

The Installation has three procedures described as below. Each procedure will be introduced in the following sections in detail.


Step 1: Installation Preparation
Obtain a floor plan
Determine the hardware and location
Determine the number of controllers according to system structure
Step 2: Hardware Installation
Installing the controller
Connecting to the door lock / open button / sensor / bell
Connecting to the alarm input / output
Connecting to the card reader
Connecting to the computer through the networkMount a backup battery in the enclosure
Step 3: Software Setup / Configuration
Log in controller built-in software through IE on computer
Set user account for user software
Set controller and other equipment
Set holidays, shifts and door control rules
Log in card and set card attributes

2.1 Installation Preparation

Before installation, users are advised to collect information properly which will make the installation more smoothly and helps to reduce time and energy cost. For professional constructors, the information below will be of great use.

2.1.1 Obtain a Floor Plan

Obtain a floor plan of the building in which the access control system is to be installed.

Obtaining a floor plan helps the installer determine what components need to be installed, and where. It also is essential in determining the length of cable needed to connect readers to the controller. A floor plan can be a blue print of the building, a design, or simply a drawing of the facility. Any document showing the footprint of the building can be used. The dimensions are important to note, especially when determining cable lengths. A floor plan may be obtained from your local city hall.

2.1.2 Determine the Hardware and Location

Determine which hardware to use and where it will be installed. This is the most crucial step in the preparation stage. First, determine how many access points, or doors, need to be managed by the access control system. These access points will control the security of the facility, and can limit the entry and exit to and from any given area of the building. After deciding which doors need to be controlled, the user must also determine the level of security needed at each door. There are many ways to manage each door, using different resources. These resources include, but are not limited to: proximity readers, mag strip readers, relays, and request to exits. A few common door configurations are described below:

- **One Set of NAV Controller+ One Reader – The Basic Door Entry Control**

The most basic configuration involves one NAV controller, a reader and an electric strike. In this configuration, a person presents a card to the reader, and is either granted or denied access. The electric strike unlocks if the system grants access. Another variation of this scenario involves setting the system up to monitor whether the door is open, which allows the system to protect against propped open doors, or doors being held open for too long.

- **One Set of NAV Controller+ One Reader + One Door Open Button – Control of Exit**

Adding a door open button to the above scenario allows the system to control when to allow people to exit through a door. The door open button equipment includes a button which has to be pressed when a card holder exits, or a door sensor. The equipment should be arranged on the secure side of the door.

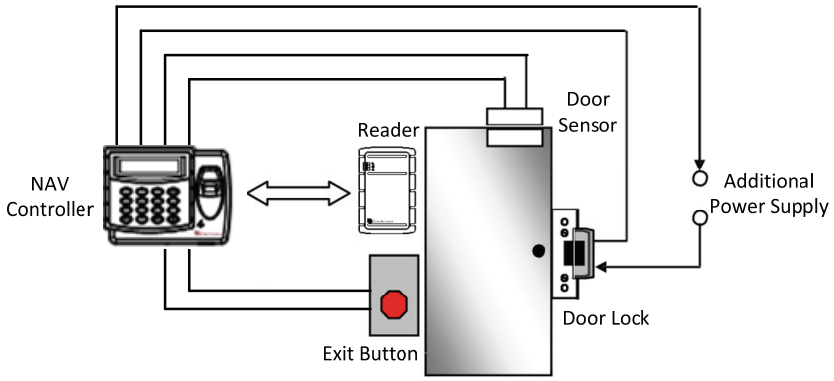


Figure 2-1

- **One Set of NAV Controller+ Two Readers – Control of both Entry and Exit**

When the security grade is relatively high or the administrator requires the card holders to get in or out at fixed time or date through specific door, two sets of EFC301 are needed. Additional installation of one set of EFC301 on the side of the door requires the card holders to swipe the card when exiting and entering. This rule has more reliable security regarding who can enter and who can exit and the administrator canal so master the entry and exit time of card holders.

2.1.3 Determine the Number of Controllers/ Modules According to System Structure

Determine how many controllers / modules and network interface are required.

1. Each NAV controller can accommodate up to 8 readers. If the system to be installed requires more than 8 readers, additional controllers are necessary. E.g. Flex series controllers.
2. If one or more controllers are installed at a different location, then the system computer is to be installed, and an Ethernet interface is required to connect over the internet. An Ethernet interface may also be used in locations at which the controllers are installed a long distance away from the system computer. Software is required to manage these NAV controllers.

2.2 Hardware Installation

After the preparation work is finished, user can start installation. This chapter mainly introduces how to install the hardware part, which is divided into six steps:

1. Mounting the enclosure (optional) and controller.
2. Installing and connecting the readers.
3. Connecting to door lock, sensor and open button.
4. Connecting to the alarm input / output.
5. Connecting to the computer.
6. Mounting a backup battery in the enclosure (optional).

2.2.1 Mounting the Enclosure (Optional) and Controller

The NAV controller should be installed in an easily-accessible position. However, it should be noticed that the controller is the core part of the entire system and can be used to change database. After the installation site is selected, a relative secure clean position in which the administrator is easy to operate should be selected.

Due to the controller is an essential part of the access control system. It is recommended to mount the NAV controller in a metal enclosure (EPN-871-B). If you are using the enclosure, additional AC power supply is required. The enclosure uses a 24V AC power supply with a built-in 15V DC converter.

If the system requires additional door or alarm modules, install them in the controller before mounting the controller in the enclosure or on the wall.

Note: If the screw holes of the controller do not line up properly with the enclosure, some filling may be required for adjustment.

1. Use the supplied mounting template to position the holes for the support frames and then mount the two support frames on a wall.

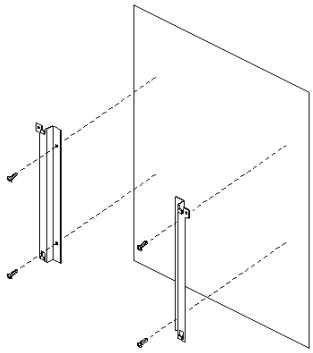


Figure 2-2

Note: If using the metal enclosure, use the four pre-drilled holes on the back wall of the enclosure and then mount the two support frames on the interior of the enclosure.

2. Mount the controller base board to the support frames.

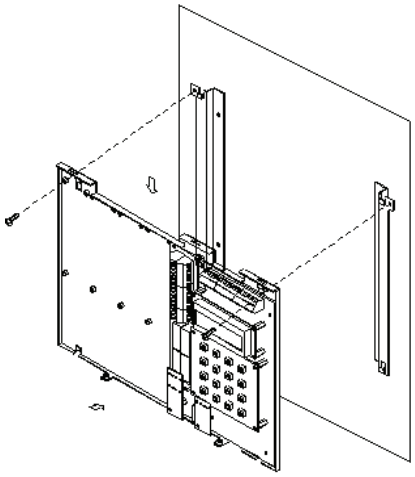


Figure 2-3

a. Place the controller base board on the support frames. Line up the four latches on the support frames with the holes on the controller base board. Once lined up, slide the controller base board down to secure it in place.

b. Secure the controller base board to the support frames using the supplied two screws.

3. Install and mount additional door modules or the alarm module.

Note: The controller can hook up to 4 door modules and only 1 alarm module. Each door module is cascaded to its left side module till the main module. The door modules and the alarm module can be placed in any sequence.

a. Connect the pins on the lower right corner of the new module to the connector on the bottom left corner of the installed module. Make sure that the pins fit snugly into the receiving module.

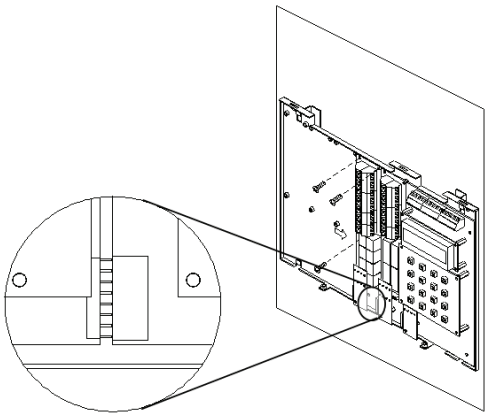


Figure 2-4

b. Secure the module to the controller base board using the three screws provided in the module package.

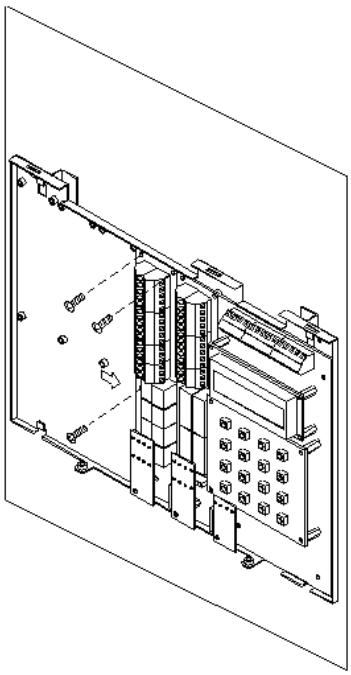


Figure 2-5

The Reader / Door Index Conversion

The index conversion of readers is displayed as below. The readers / doors are counted 1 to 8 from right to left.

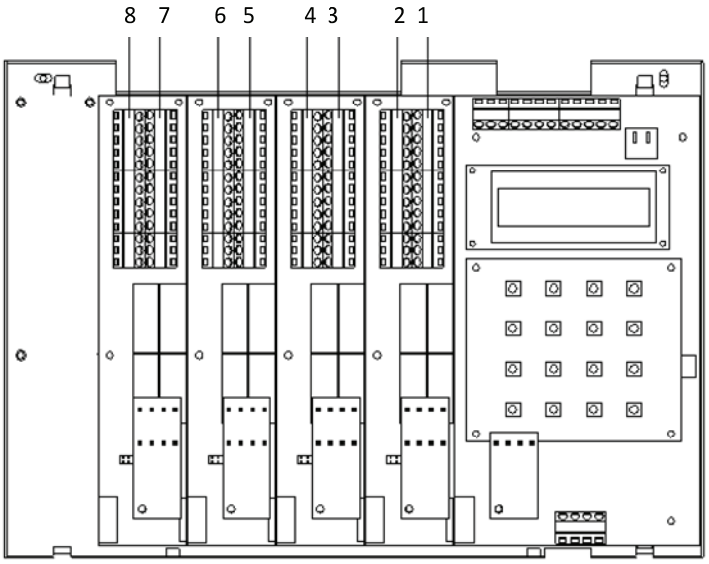


Figure 2-6

4. Placing back the cover of controller.
   a. The cover has two latches on the interior of the top horizontal edge. Place these latches in the corresponding holes on the top horizontal edge of the controller base board.

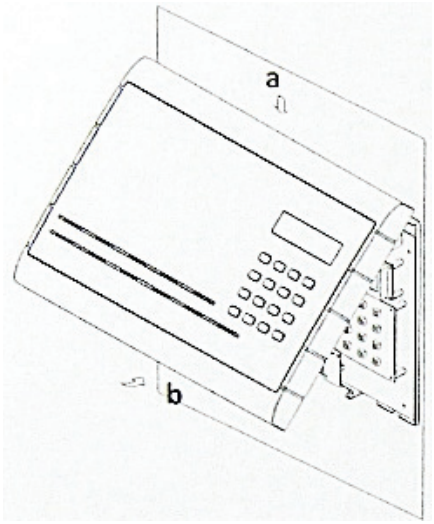


Figure 2-7

   b. Once the latches are in place, the bottom portion of the cover will fit easily over the rest of the controller base board.
   c. Secure the cover to the controller base board along the exterior of the horizontal bottom edge.

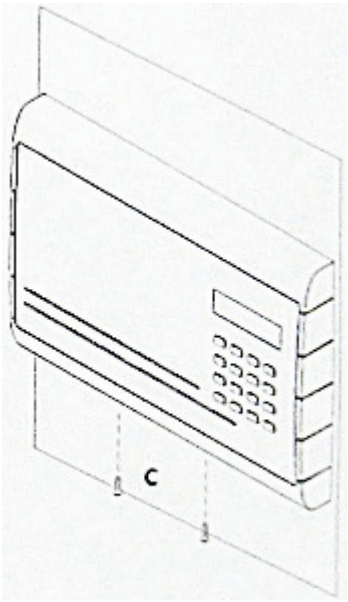


Figure 2-8

2.2.2 Installing and Connecting the Readers

The readers must be mounted near each door and connected directly to the door module(s) in the controller. Each door module can control up to two readers. The supported reader formats are Wiegand and RS-232.

RS-232 Connection

Connect the RS-232 wires from the reader to the terminal block on the door module. You can either connect the wires from the reader to **Pin 3 ~ 7** (Door 1) or **Pin 19 ~ 23** (Door 2) on the terminal block.

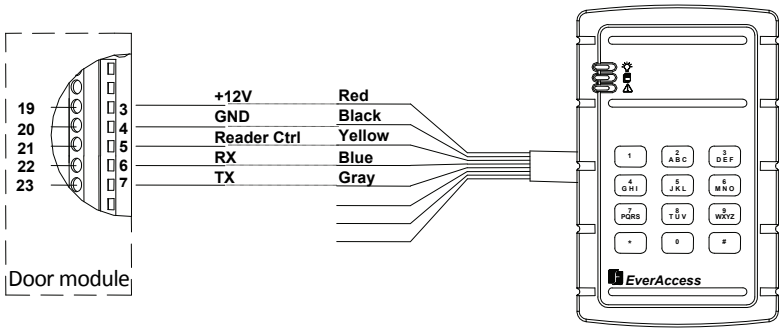


Figure 2-7

Wiegand Connection

Connect the Wiegand wires from the reader to the terminal block on the door module. You can either connect the wires from the reader to **Pin 1 ~ 5** (Door 1) or **Pin 17 ~ 21** (Door 2) on the terminal block.

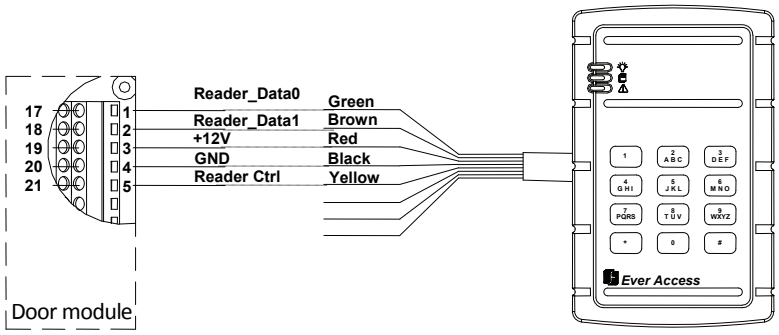


Figure 2-8

Each door module can provide +12V voltage for two readers. Twisted cable is recommended to connect the controller and readers. The maximum transmission distance between the reader and controller depends on the gauge of the cable and the specification of the reader. Please read the reader user manual carefully before installing the cable for the readers.

Note: It is strongly recommended to use one connection format in a multi-reader system, i.e. all the readers are connected to the door modules through RS-232 or Wiegand connection. Multiple connection formats could cause compatibility problems to the system.

2.2.3 Connecting to the Door Lock, Sensor and Open Button

Connecting to the Door Lock

The Electric strikes and magnetic locks are used to keep doors locked unless the system grants access or the user sets the doors to remain unlocked. One strike or magnetic lock is required for each door. These locks must be powered separately from the readers. The mounting instructions for strikes and magnetic locks vary depending on the manufacturer and type of lock. Please consult the instructions included with the door hardware when installing. Once the locks are installed, follow the instructions below to connect them to the controller.

- **Electric Strike**

  Connect the wires from the electric strike to the terminal block on the door module. You can either connect the wires to **Pin 11 and 12** (Door 1) or **Pin 27 and 28** (Door 2) on the terminal block.

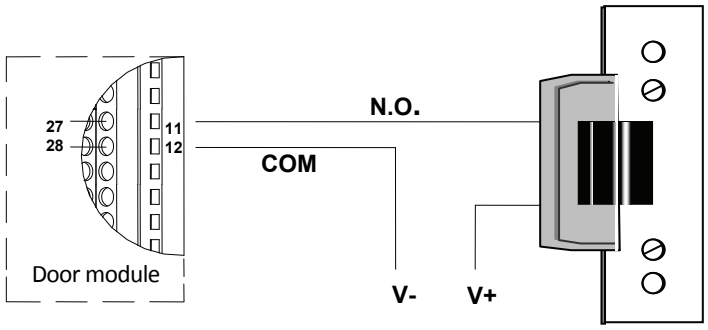


Figure 2-9

- **Magnetic Lock**

  Connect the wires from the magnetic lock to the terminal block on the door module. You can either connect the wires to **Pin 12 and 13** (Door 1) or **Pin 28 and 29** (Door 2) on the terminal block.

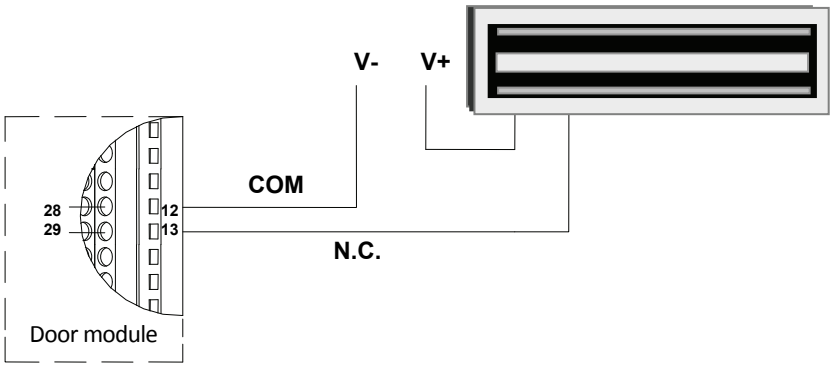


Figure 2-10

Note:

1. The maximum current output of the door lock relay is 5A. If the current of the door lock is over this value, an external power relay will be required.
2. When using a DC power source to power the lock, connect the positive lead to V+. When using an AC power source, the leads are interchangeable.

Connecting to the Door Sensor

Connect the wires from the door sensor to the terminal block on the door module. You can either connect the wires to **Pin 9 and 10** (Door 1) or **Pin 25 and 26** (Door 2) on the terminal block.

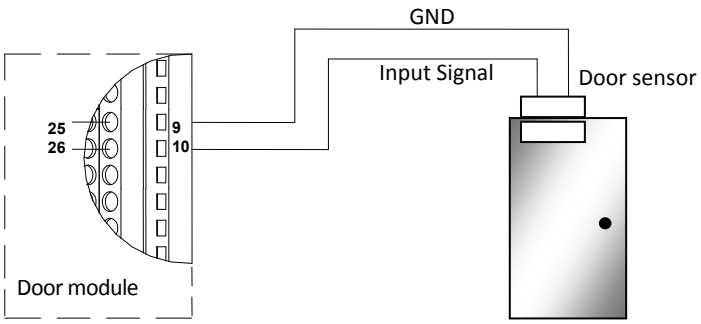


Figure 2-11

Connecting to the Door Open Button

Connect the wires from the door open button to the terminal block on the door module. You can either connect the wires to **Pin 8 and 9** (Door 1) or **Pin 24 and 25** (Door 2) on the terminal block.

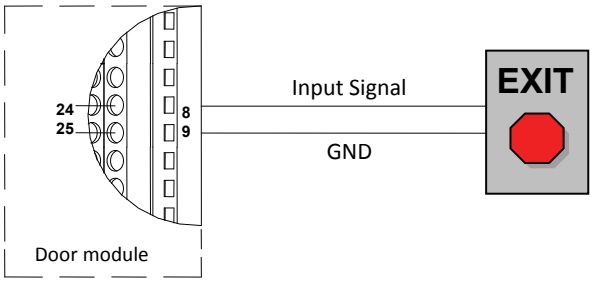


Figure 2-12

2.2.4 Connecting to the Fire Alarm/ Alarm Input

You can either connect the alarm inputs to the main module or the alarm module.

- **On the Main Module**

  The main module provides two general alarm inputs, connecting to **Pin 1** and **2** or **Pin 2** and **3** on the terminal block. The GND terminal is shared by these two input signals. Both inputs can be configured as either fire alarm input or general alarm input.

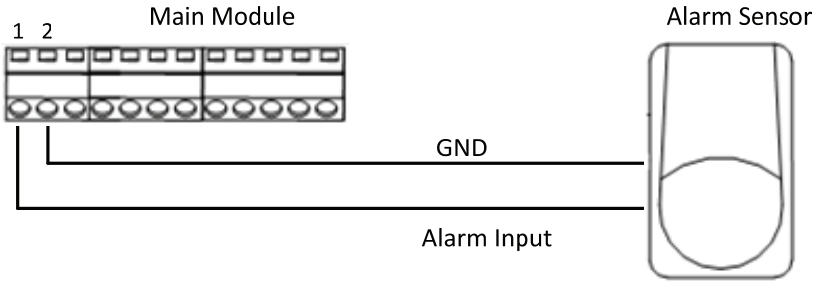


Figure 2-13

- **On the Alarm Module**

  The alarm modules provide 8 alarm inputs. The alarm input pins provided by the alarm module includes Pin 1, 3, 4, 6, 19, 21, 22, 24. For details on pin assignment, please refer to *1.6.2 Terminal Block and LEDs on Alarm Module*. Following is an example on connecting the alarm input to the alarm module.

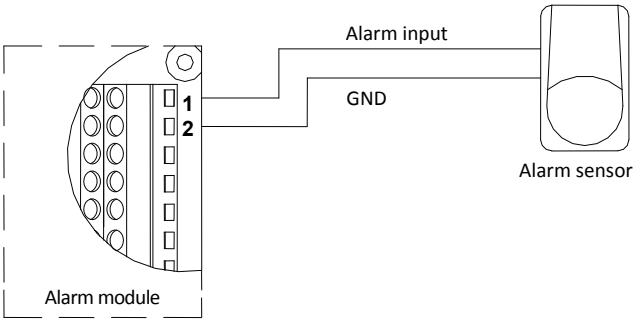


Figure 2-14

2.2.5 Connecting to the Fire Alarm/ Alarm Output

The alarm modules provide 8 alarm outputs. You can assign the corresponding relay status to the different events. There are three terminals: **COM**, **NO** and **NC**. The wiring depends on the alarm device. Please read the user manual of the external alarm devices before wiring. Following are examples on connecting the alarm output to the alarm module. For details on pin assignment, please refer to *1.6.2 Terminal Block and LEDs on Alarm Module*.

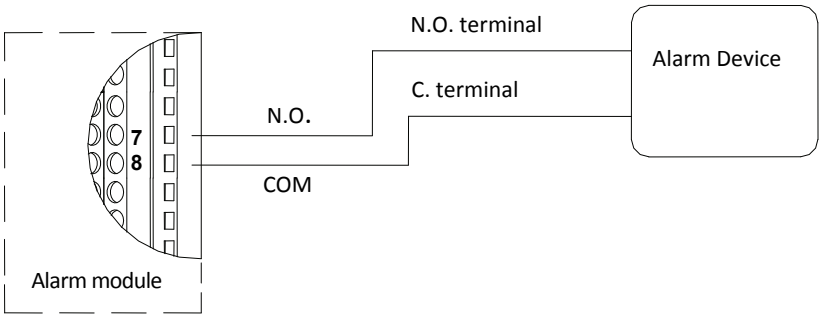


Figure 2-15

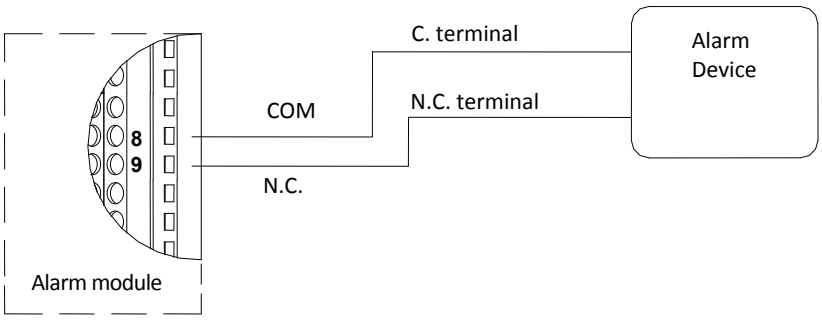


Figure 2-16

2.2.6 Connecting to the Computer through the Network

User can carry out basic setting through the keypad on the EFC301 controller or connection with the computer via TCP/IP. User can carry complicated system administration by accessing the embedded system in the controller through various browsers.

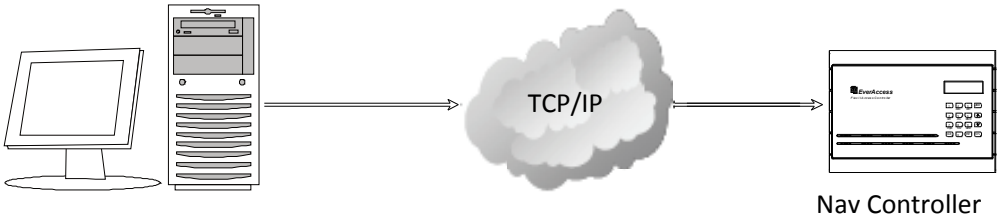


Figure 2-17

2.2.7 Mounting a Backup Battery in the Enclosure (Optional)

You can optionally connect a backup battery in the enclosure to provide backup power to the controller. Once the battery is installed, it will charge off the external power until it is needed, at which time it will automatically be used to power the system.

Connecting to the Backup Battery

Connect the wires from the backup battery to the terminal block on the main module. Connect the positive lead to **Pin 15** and negative lead to **Pin 16** on the terminal block of the main module.

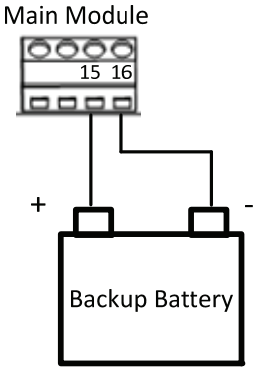


Figure 2-18

If a backup battery is connected, the controller will automatically switch to backup power in the event that the external power is lost. The backup battery will charge while external power is being supplied.

In general, the larger the battery capacity, the longer it can support the controller. A 12AH battery can provide 4 hours of energy for a controller containing 4 door modules, one alarm module and 8 readers.

Chapter
3

3. System Architecture and Connections

EverAccess® NAV Controller runs the embedded Linux and includes the built-in browser-based management software. No dedicated computer needs to be running to capture and store the events. Users can access and manage the controller or the system from any computer on the network.

This chapter introduces the 3 types of system architectures in order of system scale. Additionally, the RS485 Bus extension is introduced for extending more door controls with EverAccess Flex controllers.

3.1 Small System for 8 Doors

As introduced in chapter 1, NAV Controller provides a flexible, modulated installation up to 8 doors or readers directly. No additional controller or computer needed.

The network settings can be configured directly from the LCD and keypad on the controller. As long as the network settings are correct, users can access it by typing the controller IP address in the browser from a computer on the network. The built-in browser based software will provide the full comprehensive functions to manage and monitor the system.

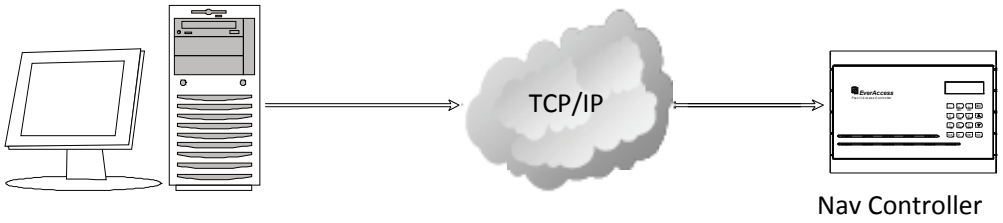


Figure 3-1 Connecting the Controller to a PC

3.2 System for 256 Doors

Each NAV Controller can connect and control up to 31 EverAccess Flex controllers via RS485 bus. Each Flex controller can hook up to 8 doors/readers, so total 256 doors/readers can be controlled under the architecture of one NAV Controller plus 31 Flex controllers.

Users can connect to the NAV Controller via a computer to remotely review, and monitor all the events on NAV and Flex controllers. Users can also all 31 Flex controllers from the browser-based management software.

The system structure is illustrated in the below figure:

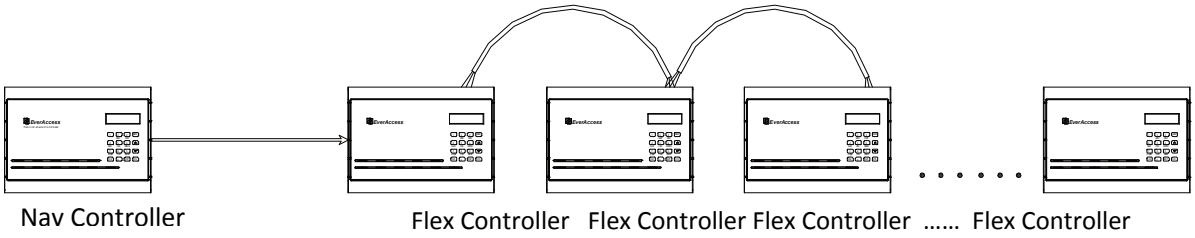


Figure 3-2 System Structure for 256 doors

3.3 System for More theN 256 Doors

Each NAV Controller can control up to 31 Flex controllers. And multiple NAV Controllers can be controlled and communicate with a Navigation software central server. Navigation software is the enterprise level software to manage middle to large scale access control system. Navigation software can be installed as central server mode or node server mode. All NAV Controllers can synchronize data and events to the central server. As a result, a larger scale system can be built with many NAV Controllers (each can control 31 Flex controllers) under the Navigation software. This large scale system is illustrated in the below figure:

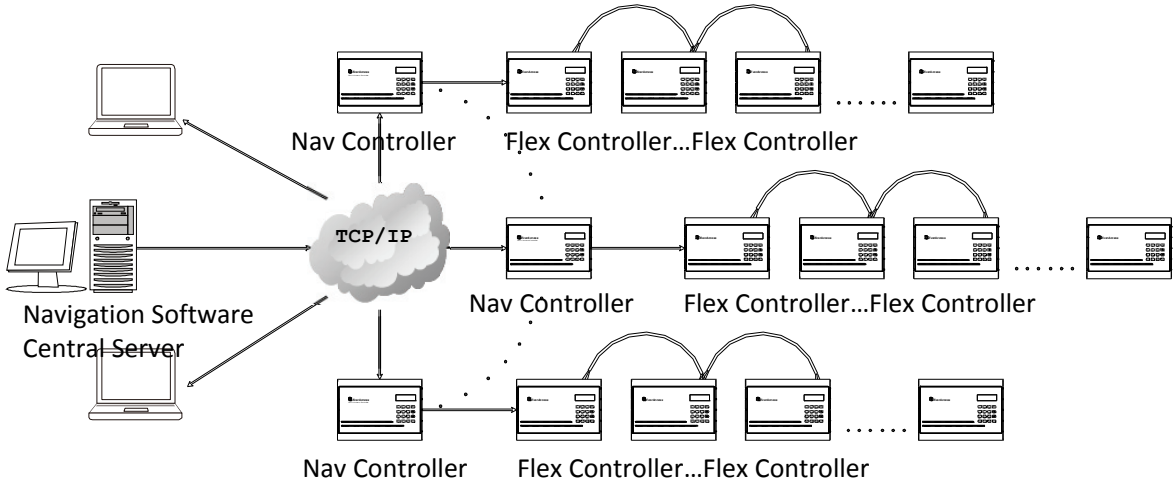


Figure 3-3 System Structure for more than 256 doors

3.4 RS485 Bus Extension

NAV Controller can connect multiple Flex controllers via RS485 bus. It is shown in the below figure:

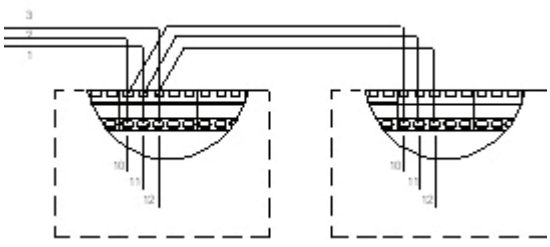


Figure 3-4 Connections to Multiple Controllers via RS485

In order to correctly transfer data, the controllers on the RS485 bus must be connected in a daisy chain format, as shown in Figure 3.5.

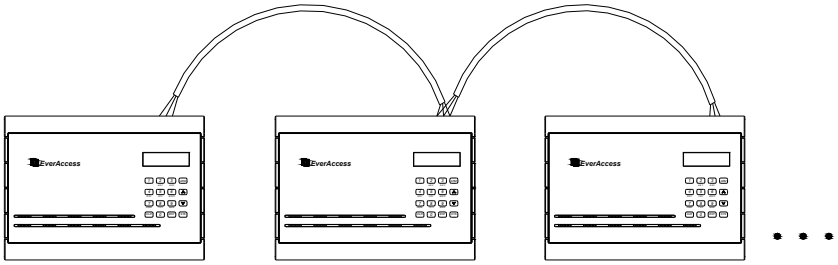


Figure 3-5 The Daisy Chain Connection Controller to Controller

Two common INCORRECT connection methods are displayed in Figure3-6 as well.

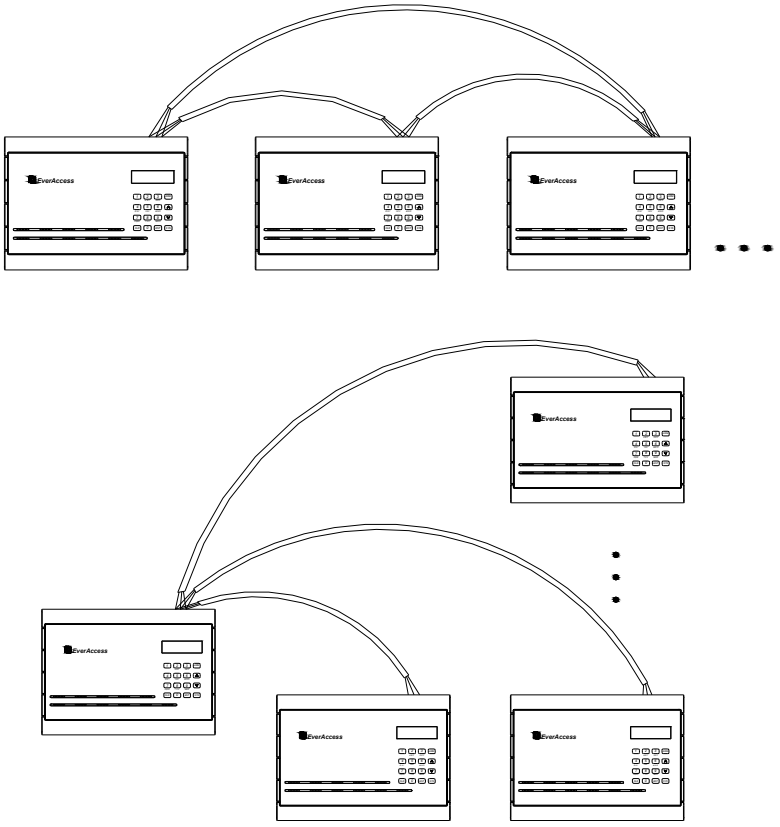


Figure 3-6 Two INCORRECT Connections

Chapter 4

4. Starting Up the Controller

4.1 Connecting to Power

You can power the NAV controller by connecting the power source to Pin 13 and 14 on the terminal block on the main module.

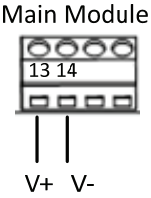


Figure 3-1

The voltage range of the NAV controller is between DC 11V and 16V. The maximum current is 500mA. If the backup battery is connected to the controller, a power supply with DC 15V is required. The power supply in the enclosure is DC 15V. In addition, the controller provides a 12V power supply for the readers. It should be noted that if a controller powers multiple readers, the current draw will be increased. The total current draw can be calculated as below:

Current (controller) **= 500 + Current** (reader) **x Number of Readers**

Important Tips:

1. The voltage supply should be located no more than 2 meters from the controller.
2. The electric locks and alarm devices must be powered separately. The controller's power supply can power the controller with the mounted modules and the readers only, but **not** the locking hardware nor the alarm devices.

4.2 Restoring the Controller

To restore the controller to the factory default settings, switch the power on while holding the **Reset** button on the main module.

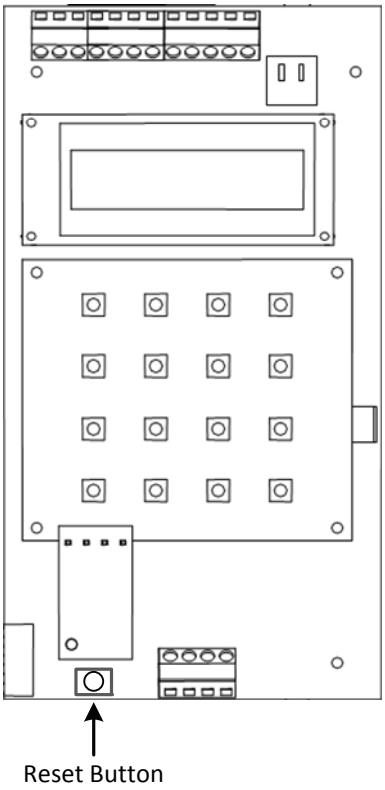


Figure 4-2

4.3 Before First Use

Before first use, please follow the instructions below:

1. Set up the IP address, date and time of the controller.
2. Set up the controller network settings.
3. Configure reader properties.
4. Configure alarm settings.
5. Configure door settings.
6. Configure date types and schedules.

Chapter 5

5. Controller Configuration and Operation

This chapter introduces system functions and their corresponding operations. Most basic operations can be performed on EverAccess® NAV Controller keypad. Some advanced functions require the built-in browser-based management software. Please refer to the later chapters for more details.

5.1 General Operation Guideline

The Controller's 4x4 Keypad is shown above:

Press SYS to enter to the system menu

Press ARM to arm or disarm the system, and reset the alarm

Press ∧ and ∨ to toggle between the same level menu

Press ∧ to move the digit input position to left when inputting numbers

Press CLR to cancel or exits back to the higher level menu

Press ENT to confirm the operation

5.2 Home Screen

After the system installation is complete, the controller LCD will display the current date and time. This display is the home screen (also called default screen in this manual), and will be displayed until the user logs in to the system configuration by entering a password.

```
2010-06-18
FRI 09:38
```

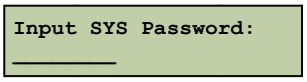
After one minute of inactivity, the controller will automatically log the user out, and back to the home screen.

5.3 Direct Operations from Keypad

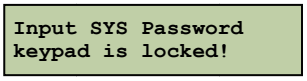
This section introduces the functions that can be accessed directly from the keypad on the NAV Controllers.

5.3.1 Enter System Configuration

Press SYS on the keypad will bring up a prompt to enter a password, as shown below:



Input the system password and press ENT. If an incorrect password is entered three times successively, the controller will alarm automatically and lock the keypad for one minute, shown as following:

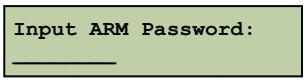


The factory default password is 000000. When Logging into the system, pressing the CLR key in each menu level will log the user out.

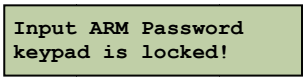
Note: It is highly recommended to secure the controller, change the default PIN after the first login, and keep the password in a safe place.

5.3.2 Enter Arm/Disarm Menu

Press ARM button under the default date/time screen, the below screen will pop up to prompt users to input the arm PIN:



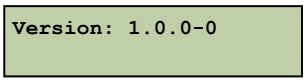
After entering the arm PIN, press ENT to confirm and input the ARM menu. The default arm PIN is 00000000. If an incorrect arm PIN is entered three times successively, the system will alarm automatically and lock the keypad for a period of one minute, shown as the below sample window:



Note: It is highly recommended to secure the controller, change the default PIN after the first login, and keep the password in a safe place.

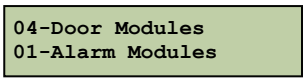
5.3.3 Display Firmware Version

Press 0 to show the version information of the currently installed firmware. An example is shown below:



5.3.4 Display the Number of Installed Modules

Press 1 to show the number of installed door modules and alarm modules. For example, 4 door modules and 1 alarm module are installed in the controller. The example window is shown below:

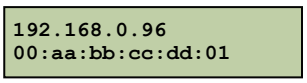


5.3.5 Display the Current Card and Event Number

Press 2 to show the number of currently enrolled card and currently stored events. For example, right now the controller stored 100 cards and 36,555 events. The example window is shown below:

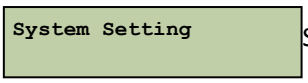
5.3.6 Display the Controller IP Address

Press 3 to show the IP address, MAC address of the controller. An example window is shown below:

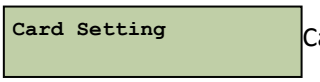


5.4 Level One System Configuration Items

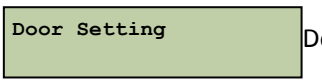
The first level menus are displayed after entering the system menu. Use ∧ and ∨ to toggle between menu options. The first level menu items are shown below:



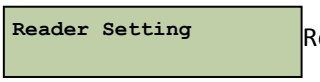
System Setting Menu



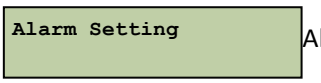
Card Setting Menu



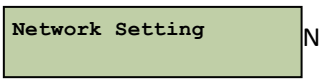
Door Setting Menu



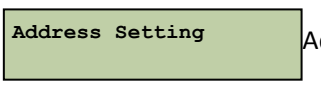
Reader Setting Menu



Alarm Setting Menu



Network Setting Menu



Address Setting Menu

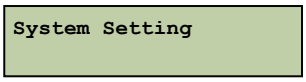
Once the desired item is displayed, press ENT to enter into the corresponding menu. And press CLR in the corresponding menu to return the level one menu.

5.5 System Setting

In the System Setting menu, the user can set basic functions, including date format, system date, time, password, auto daylight saving, system PIN, arm PIN, language, backlight, event erasing and load factory default.

5.5.1 Enter System Setting Menu

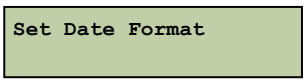
The following window appears after entering the system menu:



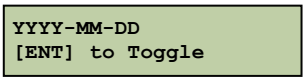
Press ENT to enter System Setting menu. Use ∧ and ∨ to choose from different menu options. All menu options in the System Setting Menu are introduced below.

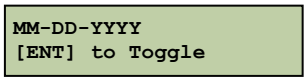
5.5.2 Set Date Format

The user can choose between two date formats: 'MM-DD-YYYY' or 'YYY-MM-DD'. To change this option, use the arrow keys to display "Set Date Format", and press ENT once the window below is displayed.



The current date format used will appear. Press ENT to toggle between two formats. Press CLR to exit. The selected format is the one shown on window when exiting.

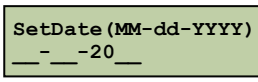




5.5.3 Set Date

Press ENT at the window below to set the date.

The LCD will display the following menu. Use the numerical keys to input the current date as a six-digit number: (MM-DD-20YY). The year must be in the range 2000-2038. Press ENT to confirm the new date.

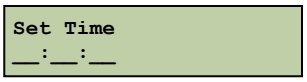


The date and time can be set either at the controller or from the built-in management software remotely.

5.5.4 Set Time

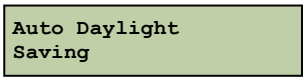
Press ENT at the below window to set the time.

The LCD will display the following menu. Use the numerical keys to input the current time as a six-digit number (HH: MM: SS). The time must be in the range 00:00:00--23:59:59. After entering the time, press ENT to confirm.

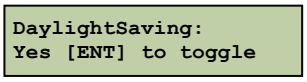


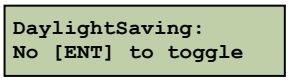
5.5.5 Auto Daylight Saving Time

Press ENT at the below window to adjust the settings for Auto Daylight Savings:



Press ENT to toggle the setting between Enabled/Disabled, Press CLR to exit



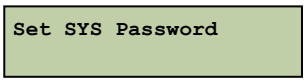


When auto daylight savings is turned on, set the auto daylight start/end time from the built-in management software remotely.

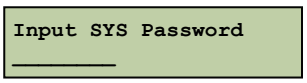
5.5.6 Set System PIN

A System PIN must be entered before the user can make management changes via the controller keypad. The factory default System PIN is 00000000. It is recommended that the password is changed after the initial log-in for maximum security. Be sure to secure the new password; if lost, the system can only be accessed after purging all stored data using the reset button on the main board.

Press ENT at the below window to set system PIN.



The LCD will display the following menu.



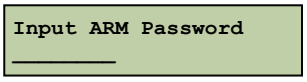
Enter a new system PIN. Enter it a second time to confirm. Press ENT to set the new system PIN. Pressing CLR at any time will exit the menu without changing the system PIN.

5.5.7 Set Arm PIN

Arm PIN must be entered before the controller can be armed or disarmed via controller keypad. The factory default arm PIN is 00000000.

Press ENT at the window below to set arm PIN.

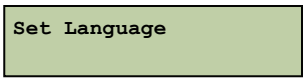
The LCD will display the following menu.



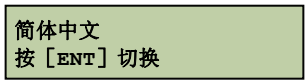
Enter a new arm PIN. Enter it a second time to confirm. Press ENT to set the new arm PIN. Pressing CLR at any time will exit the menu without changing the arm PIN.

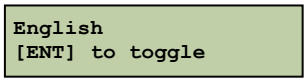
5.5.8 Set Language

Press ENT at the below window to adjust the language setting:



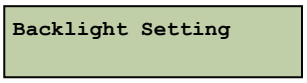
Press ENT to toggle among Chinese, English and Russian, Press CLR to exit. The selected language is the one shown on window when exiting.



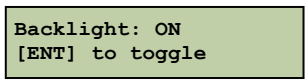


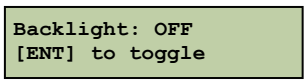
5.5.9 Backlight Setting

Press ENT at the below window to change the backlight setting



Press ENT to toggle between enabling and disabling backlight. Press CLR to exit

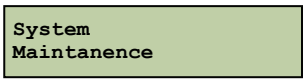




5.5.10 System Maintanence

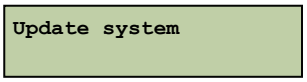
NAV Controller supports two ways to update firmware, backup and restore database: via USB drive or FTP. This section introduces how to use system maintenance with a USB drive.

Press ENT at the below window to enter to the system maintenance menu.

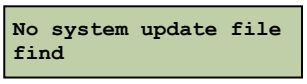


5.6.4.1 Firmware update

Plug the USB drive that contains the firmware file into the USB port of the controller. Press ENT at the below screen of system maintenance menu to start the firmware updating process.

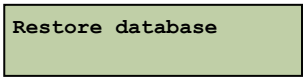


The controller will show the below screen if no valid firmware is found from the plugged USB drive.

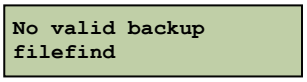


5.6.4.2 Database restore

Plug the USB drive that has the previous backup database file into the USB port of the controller. Press at the below screen to start database storing process.



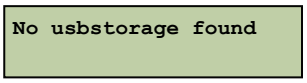
If no valid database data available, the controller shows the below information:



5.6.4.3 Database backup

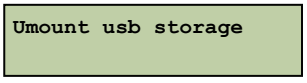
Plug the USB drive into the USB port of the controller. Press ENT under the below screen to backup the database to the USB drive:

If no USB drive presented when the menu item is selected.

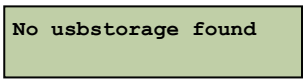


5.6.4.4 Unmount USB storage

USB drive can be hot swapped, but sometime the data will be loss caused by pulling out directly. It is safer that removed from the controller. Press ENT under the below screen to unmount the USB drive when finishing backup and restoring the database from the backup file on USB drive:



If no USB drive presented when the menu item is selected.



5.5.11 Erase All Events

The controller will record all events that occur, beginning immediately upon powering on. These events can be purged by following the instructions below. The old records will be automatically overwritten when storage space is full (1,000,000 events max.).

Press ENT at the window below to erase all events.

```
Erase All Events
```

LCD will prompt the user to confirm the action:

```
Are you sure?
[ENT] to continue
```

Pressing ENT will result in all events being permanently erased.

⚠ **Caution**: this operation will permanently delete ALL events from the controller database. This operation is NOT undoable.

5.5.12 Load Factory Default

This function is used to reset all settings to factory set default values.

Press ENT at the window below to reset all settings.

```
Restore Factory
Settings
```

The LCD will prompt the user to confirm the action. Press ENT to confirm and perform the reset action.

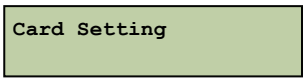
⚠ **Caution**: this operation will recover all the settings to the factory default. This operation is NOT undoable.

5.6 Card Setting

Card setting can be configured using either the controller or the built-in management software. Using the built-in management software is the easiest way to enroll cards. However, enrolling at the controller can be useful if the controller is offline. The process is described below.

5.6.1 Enter Card Setting Menu

Under the System Menu, press V once to bring up the following window:



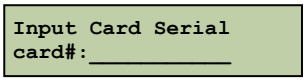
Press ENT to enter to the Card Setting menu. Use ∧ and ∨ to choose from different menu options. All menu options under the Card Setting menu are introduced below:

5.6.2 Add Cards

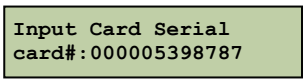
When a new card is added, the controller will automatically assign an index number in the order of enrollment. The index number here is not related to the card number in the software. Users do not need to take care of this number.

Under the Card Setting menu, press ENT at the window below to add a card:

Press ENT and enter a serial number on the card, as shown below:



User input card serial number, or swipe card via system reader, system reader will automatically read the card serial number to the controller.



Press ENT to confirm and the system will add the card to the controller database. The user can also present the card at the system reader at this time, which will automatically acquire the index number of the new card, show the card number and add it to the controller. It will show “card exists already” if the same card number is in the database already.

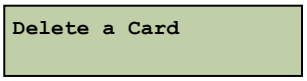
5.6.3 Delete Cards

The user can directly delete an individual card with a specific index or card number from the controller, or delete all cards at once. Under the Card Setting menu, press ∨ once to bring up the following window:

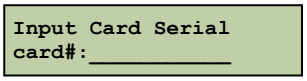
Press ENT to enter to the submenu for the following two methods of deleting cards.

5.6.4.5 Delete a Card

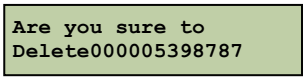
The controller can delete a card according to its serial number, which is printed on the face of each card. At the following window:



Press ENT and the system will prompt the user to enter a card serial number, as shown below:



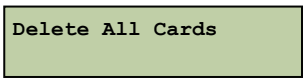
After entering the serial number, press ENT to delete this card. The system will prompt users to confirm again like the below screen:



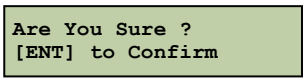
Press ENT to confirm or press CLR to exit from the “delete card” menu.

5.6.4.6 Delete All Cards

All cards can be deleted at once. At the following window:



Press ENT and system will prompt the user to confirm deletion:



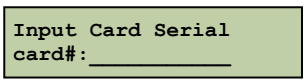
Press ENT again to delete all cards.

⚠ **Caution**: this operation will permanently delete ALL cards from the controller database. This operation is NOT undoable.

5.6.4 Set Card Properties

Under the Card Setting menu, press V twice to bring up the following window:

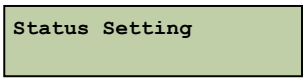
Press ENT and system will prompt the user to enter serial number, as shown below:



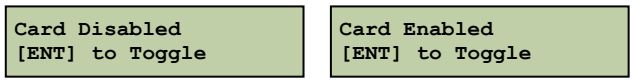
After entering the serial number, press ENT to enter to the submenu for setting card properties. Each card has 6 properties that can be modified. Use ∧ and V to choose desired properties.

5.6.4.7 Status Setting

A card can be set as enabled or disabled at the following submenu:

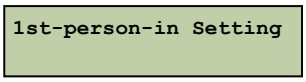


Press ENT and system will show the status of current card as the figure below. Press ENT to toggle between the two statuses. Press CLR to exit. The selected value is the one shown on window when exiting.



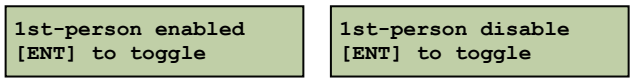
5.6.4.8 First Card Setting

A card can be set as either first card or not from the below submenu:



Note: First card property indicates if the card can trigger the scheduled door verification rules. For example, even when the doors are configured as always open during the office hour, but it will still remain locked if NO card with enabled “First card” property yet presented and gained the access to the doors in the office hour. For each day, the door verification schedule will be triggered (in this example, become to unlocked in office hour) only after a card with enabled “first card” presented and gained the access.

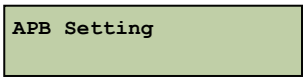
Press ENT and system will show the “First card” setting of the card as the figure below. Press ENT to toggle between ON/OFF status of the first card setting.



5.6.4.9 Anti-Passback (APB) setting

NAV Controller features the Anti-Passback (APB) function on each card. If APB is enabled, cardholder must pass the door in the alternating enter/exit. That is, if the card is swiped to access the door, then next time the card can only be allowed to exit that door. If cardholder attempts to access the same door again without first swipe the card to exit the door, access is denied and the door will not open.

At the following submenu, press ENT to enter Anti Passback setting:



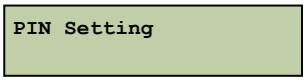
The APB status of the current card is enabled or disabled, will be displayed as shown below. Press ENT to toggle between two statuses. Press CLR to exit.

Note: Anti-Passback (APB) is an access control function whereby a cardholder is prevented from “passing back” his card to another person to gain entry into the same area twice, without leaving. Facilities are typically fitted with both Entry and Exit readers when Anti-Passback is implemented. A cardholder must alternate usage between entry and exit readers. If the cardholder attempts to pass through an entry reader twice consecutively, his access will be denied and the system will generate an illegal event when the cardholder’s card is configured as APB enabled. Be careful to enable this function in the system with only single side readers installed somewhere.

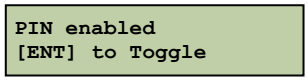
5.6.4.10 Card PIN Setting

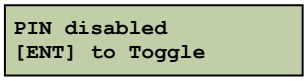
Each card in the NAV Controller is associated with an 8-digit PIN. The PIN status can be set as enabled or disabled and if enabled, A cardholder is required to input the PIN every time when enters/exit the door if the reader is a keypad reader.

At the following submenu, press ENT to enter PIN setting:



The PIN status of the current card, i.e., enabled or disabled, will be displayed as shown below. Press ENT to toggle between two statuses. Press CLR to exit.



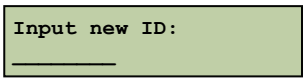


5.6.4.11 Change Card Serial Number

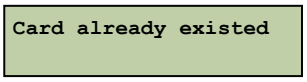
Each card in the NAV Controller has a unique serial number, it can be modify. Usually if the cardholder lost the card and doesn't want to add a new one again, it can be modified from the old serial number to the new one.

At the following submenu, press ENT to change card ID:

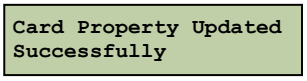
The below screen will be shown to prompt users to input new ID.



The user can either swipe the card through a system reader to get a new ID, or input it manually. Press ENT to confirm the input of new ID. If input ID already exists, the system will prompt:

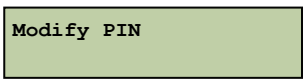


Otherwise, system will show the below information:

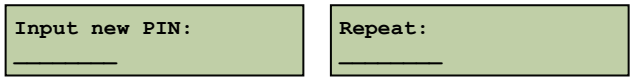


5.6.4.12 Modify card pin

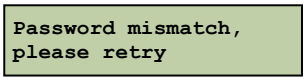
Each card in the NAV Controller system is associated with an 8-digit PIN. Card PIN can be modified from the below screen. At the following submenu, press ENT enter to Modify Card PIN.



Press ENT to prompt to input new PIN, press ENT to repeat new PIN.



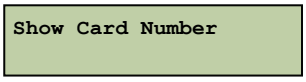
If repeat PIN is different from first time input, it will prompt,



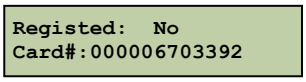
After modify, it will prompt,

5.6.5 Show Card Number

This function can be used to show the serial number of a card when it is swiped on the system reader. Under Card Setting menu, press V three times to bring up the following window:



Press ENT and swipe the card on the system reader. The serial number of the card will be displayed as shown below. Press CLR to exit.

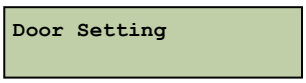


5.7 Door Setting

Every door module controls two door relays. NAV Controller can control up to 8 doors in total, defined as door 1 to 8 from right to left. According to reader setting above, users can allocate multiple readers to one single door. User can directly set door unlock time, door held open time and the door control at fire alarm on the controller.

5.7.1 Enter Door Setting Menu

Under System menu, press V three times to bring up the following window:



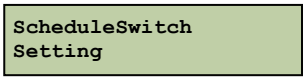
Press ENT to enter Door Setting menu. Use ^ and V to choose from different menu options. All menu options under Door Setting are introduced below.

5.7.2 Schedule Switch Setting

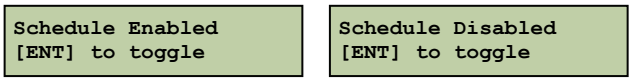
Door verification indicates the access mode when a cardholder enrolls the card on the reader in order to enter/exit the door, for example, a dual security method could require both card and PIN, or both card and fingerprint.

NAV Controller supports a comprehensive door verification schedule on each door. The door verification can be defined individually on a schedule with 10 types of date, 6 time zones on each type of date. If the user just wants to have a consistent access mode all the time every day, schedule switch can be set as OFF to have only one door verification mode, defined in the next section.

At the following submenu, press ENT to enter to the setting for door verification schedule:



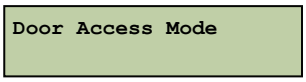
Press ENT to toggle between enable/disable door verification schedules. Press CLR to exit.



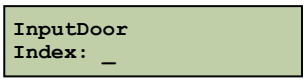
5.7.3 Door Access Mode

As described in previous section, NAV Controller will use the controller door access mode if the schedule switch is turned off. NAV Controller supports 13 types of door access modes, for example: always open, card only, fingerprint only and so on.

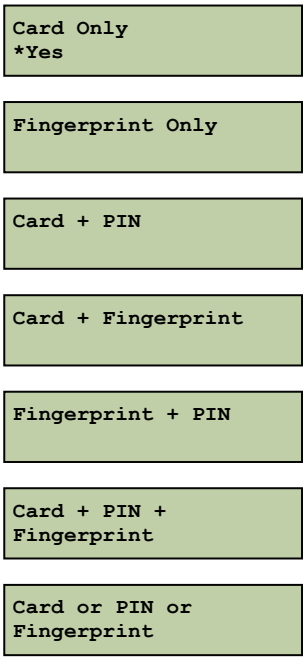
At the following submenu, press ENT to set the controller door access mode:

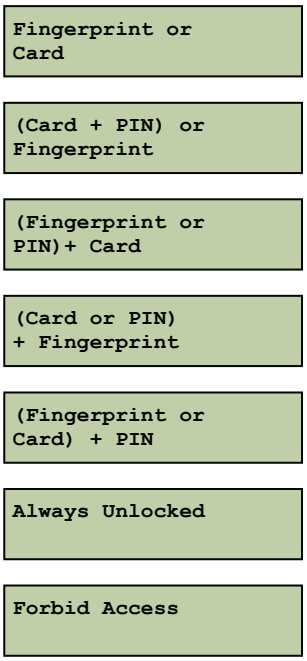


Before setting the door verification mode, users first have to select the door to be set, refer to the below window:



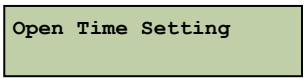
After the door number is entered, press ENT to toggle among all available door verification modes. The modes followed with a star "*" mark is the currently selected mode. All the door verification modes are listed below:





5.7.4 Open Time Setting

This sets the door open time when the card is swiped or request-to-exit button is pushed. The default time is 3 seconds. The maximum door open time supported by the controller is 999 minutes and 59 seconds. The door remains open as long as the request-to-exit button is pushed down. The door open time does not count until the button is released. In the following submenu:



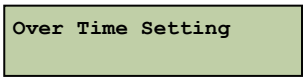
Press ENT to enter door Open Time setting. Use ∧ and ∨ to choose from different door.

Input the desired door open time: enter minutes as a 3-digit number 0~999, and enter seconds as a 2-digit number 0~59. Press ENT to confirm. Press CLR to exit without effecting any change.

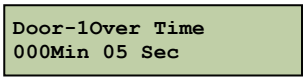
5.7.5 Over TimeSetting

Door sensor monitors the open/close status of a door. If normally open is not set by the system (door is normally considered closed), then door should close after opening for a while. It is considered abnormal if controller does not receive the door close signal from door sensor in a reasonable amount of time after the door is opened. This time period is called door hold open time or door over time. According to this setting, NAV Controller will determine whether to generate an alarm or not after the door sensor timeouts. The default value of door hold open time is 5 seconds. The maximal door hold open time supported by the controller is 999 minutes and 59 seconds.

At the following submenu:



Press ENT to enter Over Time setting. Use ∧ and ∨ to choose from different door.



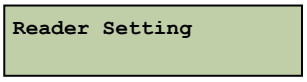
Input the desired door hold open time in the Open Time field: enter minutes as a 3-digit number 0~999, and enter seconds as a 2-digit number 0~59. Press ENT to confirm. Press CLR to exit without effecting any change.

5.8 Reader Setting

Card reader properties can be directly set on the controller, including whether the reader is keypad reader, the allocation of readers to doors, and system reader etc.

5.8.1 Enter Reader Setting Menu

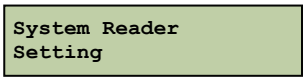
Under System menu, press ∨ twice to bring up the following window:



Press ENT to enter Reader Setting menu. Use ∧ and ∨ to choose from different menu options. All menu options under Reader Setting are introduced below:

5.8.2 System Reader Setting

System reader can be used to acquire the card's serial number when controller configures the card. User can set any reader that connects to the controller as the system reader. At the following submenu:

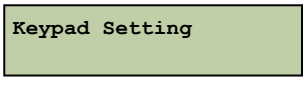


Press ENT to enter System Reader setting. System will show current status of all readers as shown below. Y means the reader is the system reader, N means it's not. By default, no reader is set as the system reader. Users have to set it manually.

Press any of the 1-8 numeric keys to change the system reader setting of corresponding readers. Press CLR to exit.

5.8.3 Keypad Setting

Keypad Setting defines whether the reader is a keypad reader. For a keypad reader, if the PIN property of the card is set as enabled, and the access rights of the door are set as card plus PIN, then the user is asked to enter password when the card is swiped on the keypad reader. At the following submenu:



Press ENT to enter keypad setting. System will show keypad setting status of all installed readers. Y means the reader is a keypad reader, and N means the reader is a non-keypad reader. By default, every

reader is set as a non-keypad reader. Flex controller will display the door number according to the number of installed door modules. In the following example, 4 door modules (8 readers) have been installed on the controller.

```
12345678
NNNNNNNN
```

Press numeric keys to toggle the keypad setting of corresponding reader. Press ENT to confirm. Press CLR to exit without effecting any change.

5.8.4 Reader to Door Allocation

NAV Controller can be flexibly configured. Readers can be allocated to different doors, and can be set as ENTER only or EXIT only. By default, each reader is allocated as ENTER only to the door with the reader's number. At the following submenu:

```
Reader to Door
Allocation
```

Press ENT to enter Reader to Door Allocation setting. System will show the allocation of the first reader to door as following:

```
Reader-1
Door-1-IN
```

Press any of the 1-8 numeric keys to allocate the current reader to corresponding doors. (This depends on the actual door modules installed on the controller) Press the same numeric key to toggle between ENTER only (IN) and EXIT only (OUT).

Press the ∧ or ∨ to select the different readers. Press CLR to exit.

5.8.5 Reader Backlight Setting

At the following submenu:

```
Reader Backlight
Setting
```

Press ENT to enter Reader Backlight Setting. As shown below, the system will show if the backlight setting of all readers are turned on or off. Y indicates ON, N indicates OFF. The default setting of backlight is OFF. Note this feature only applies the reader released after Q3, 2010.

```
12345678
NNNNNNNN
```

Press any of the 1-8 numeric keys to change the backlight setting of each reader. Press CLR to exit.

5.8.6 Set Reader LED or LCD format

At the following submenu:

```
Set Reader LED or
LCD Format
```

Press ENT to enter Reader LED/LCD format. As shown below, the system will display if the showing format of all readers are LCD or LED. Y indicates LED, N indicates LCD. The default setting is LCD. Note this feature only applies the reader released after Q3, 2010.

```
Reader LED/LCD Set
NNNNNNNN
```

Press any of the 1-8 numeric keys to change the format setting of each reader. Press CLR to exit.

NOTE: LCD format will display more information, include current time, card serial number, employee full name (if value is set), success or failure of current access verification. The screen of the reader must be an LCD, shown as following:

```
2010-06-18 FRI 09:38
000005398787
Kelly
Verify Succeed!
```

If the screen of the reader is LCD, but set the format is LED, it is shown as following:

```
OPEN
```

5.8.7 Set Card Format

At the following submenu:

```
Set Card Format
```

Press ENT to enter Card Format Setting. As shown below, the system will show what the reading card direction of all readers is. The default setting of card format is N. Note: this feature only applies the reader released after Q3, 2010.

```
CardFormat Setting
NNNNNNNN
```

Press any of the 1-8 numeric keys to change the format setting of each reader. Press CLR to exit.

NOTE: Users do not need to take care of what is the detail of this reading direction. The user just chooses the correct format when the card serial number shown on the LCD screen matching the number printed on the card self.

5.9 Alarm Setting

NAV Controller is equipped with powerful alarm functions. With alarm modules and door modules fully installed, the controller can accommodate up to 10 alarm inputs and 18 alarm outputs. In the meantime, the controller also provides a very flexible configuration. Any event can be arbitrarily allocated to single

or multiple alarm outputs. Alarm components, configuration basics, and menu settings are introduced below.

5.9.1 Components for Alarm

NAV Controller consists of two basic components: one main module and one door module. Users can additionally install three more door modules and one alarm module.

These three types of modules are all equipped with alarm function. The main module has 2 alarm inputs and 2 alarm outputs, called Main Alarm Output and Auxiliary Alarm Output respectively.

Each door module has 2 alarm outputs, which usually react to alarm events on the corresponding door. However, it can be set to react to other alarm events as well. Alarm outputs on the door module can connect up to 5A external alarm devices.

The alarm module has 8 alarm inputs and 8 alarm outputs. 8 alarm inputs can connect to external alarm input devices, such as PIR motion sensor, glass sensor and etc. 8 alarm outputs can connect up to 2A external alarm devices.

The above mentioned are physical devices providing alarm functions

User can freely define the allocation of any input to any output. The following section outlines basic concepts for events, alarm and configuration.

5.9.2 Alarm Configuration Basics

NAV Controller keeps track of all events in the access control system, either legal or illegal, either normal or abnormal. For example, access granted, access denied and so on.

Some events are critical which must trigger the alarm output, like the firm alarm input, the zone alarm input and etc. But some events are not that important to trigger the alarm output, like the denied access due to the invalid time. These settings all depend on the users' requirements. NAV Controller collects all events that might trigger the alarm output and provides the full capacity to enable or disable the alarm output on these events.

Sometimes user wants to allocate a particular event to a particular alarm output, or allocate alarm inputs in certain area to multiple alarm outputs. NAV Controller delivers all the function and flexibility user need. User can define whether certain event will trigger an alarm, and can further specify to which alarm output that event is allocated.

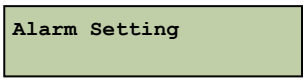
All events that might trigger an alarm are listed below:

Alarm input 0~9, unknown card, expired card, invalid card, invalid door, invalid time, card anti-pass back fail, card PIN fail, SYS PIN fail, ARM PIN fail, door forced open, door held open, reader lost, and remote alarm.

All these events can be allocated to any alarm relay output on main module, door module, and alarm module. The detailed configuration method is introduced in the following section.

5.9.3 Enter Alarm Setting Menu

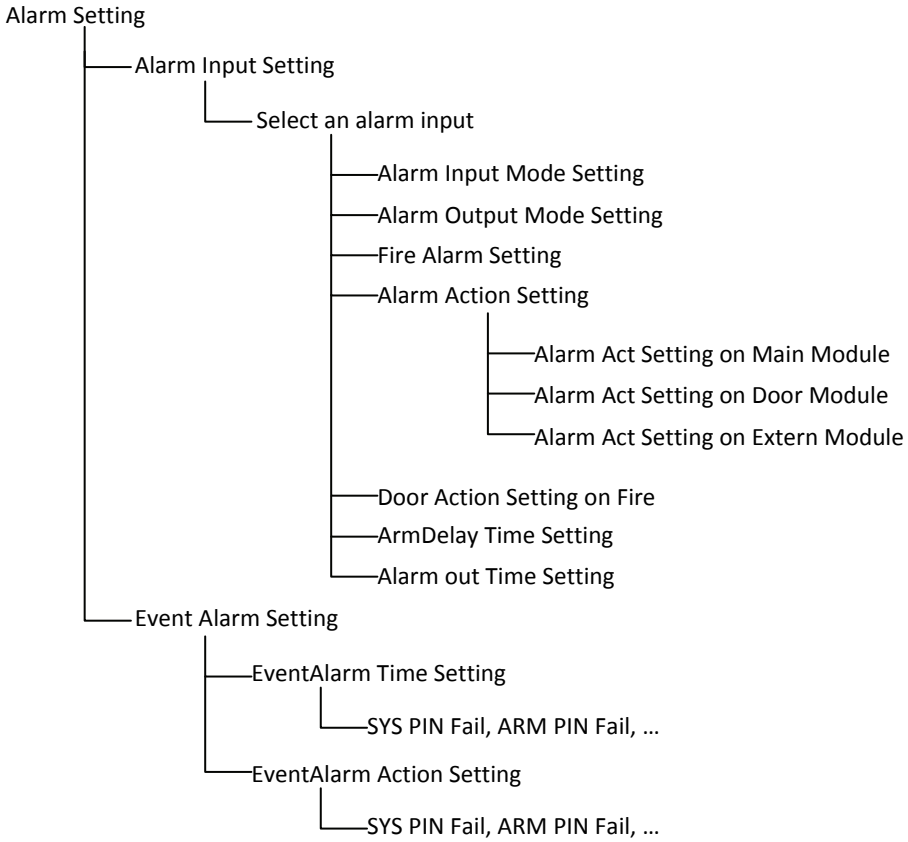
Under System menu, press four times to bring up the following window:



Press ENT to enter Alarm Setting menu. Use ∧ and ∨ to choose from different menu options. All menu options under Alarm Setting are introduced below:

5.9.4 Alarm Setting Menu Structure

There are two submenus under Alarm Setting, as shown below:

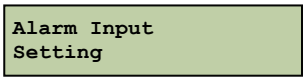

Alarm Setting
Alarm Input Setting
Select an alarm input
Alarm Input Mode Setting
Alarm Output Mode Setting
Fire Alarm Setting
Alarm Action Setting
Alarm Act Setting on Main Module
Alarm Act Setting on Door Module
Alarm Act Setting on Extern Module
Door Action Setting on Fire
ArmDelay Time Setting
Alarm out Time Setting
Event Alarm Setting
EventAlarm Time Setting
SYS PIN Fail, ARM PIN Fail, …
EventAlarm Action Setting
SYS PIN Fail, ARM PIN Fail, …

Alarm input setting menu is used to configure the settings of the physical alarm inputs on main module and alarm module, including input mode, output mode, fire alarm input, alarm output actions, door behavior under fire alarm, arm delay time, and alarm output duration.

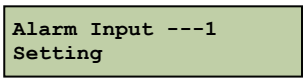
Event alarm setting menu is used to configure alarm outputs and output duration for all events on main module and door module.

5.9.5 Alarm Input Setting

From the Alarm Setting menu, go to the below window:

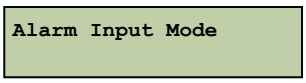


Press ENT to enter to the alarm input setting, the system will first prompt users to select an alarm input, like the below window. Total 10 alarm inputs (0-9) available in NAV Controller.

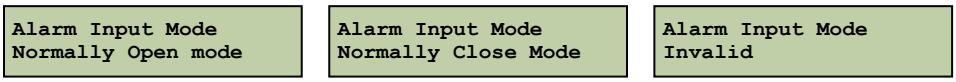


5.6.4.13 Alarm Input Mode

At the above window, press ENT to enter to the setting for alarm input #1. The 1st submenu is the alarm input mode submenu, use ∧ and ∨ to switch to other submenus.



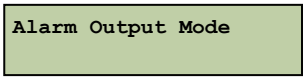
Three alarm input modes are available: N.O., N.C, and Invalid. Press ENT to toggle among the three modes.



- N.O. mode indicates the normal status (no alarm input signal) of circuit is disconnected. It will be alarmed if the alarm input is active and the circuit will be closure.
- N.C. mode is the inversed case of N.O. It means the normal status of circuit is closure. It will be alarmed if the alarm input is active and the circuit will be disconnected.
- Invalid input indicates the related alarm input is disabled.
-

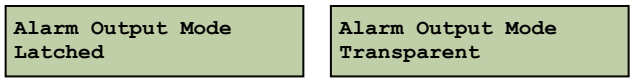
5.6.4.14 Alarm Output Mode

At the following window, press ENT to configure the alarm output mode



There are two alarm output modes: latched mode and transparent mode.

Press ENT to toggle between the two modes.



- Transparent mode indicates the alarm output will present as long as the alarm input is valid, and alarm output will disappear when the alarm input is invalid. The duration of alarm output is purely controlled by the duration of valid alarm input, not related with the timeout configuration.
- Latched mode indicates that alarm output can only be triggered by the valid alarm input after the arm delay duration. And the alarm output will be last for the specified alarm timeout duration.

5.6.4.15 Fire Alarm Setting

Under the below window, press ENT to configure the fire alarm feature of an alarm input:

```
Fire Alarm Setting
```

Fire alarm setting is used to configure other alarm inputs as the fire alarm input. Fire alarm input does not follow the arm delay time, it has the highest priority. It is triggered as long as the alarm input defined as fire alarm is configured. All 10 alarm inputs can be defined fire alarm input.

```
Fire Alarm
Fire alarm input
```

```
Fire Alarm
Other alarm input
```

5.6.4.16 Alarm Action Setting

Alarm Action Setting is used to configure the allocation between the physical alarm input and the output on main module, door module and alarm module.

Press ENT to configure alarm action setting when the following window appears.

```
Alarm Action Setting
```

NAV Controller provides total 18 alarm outputs: 2 alarm outputs on main module, 8 alarm outputs on door module, 8 alarm outputs on alarm module. They are allocated in 3 submenus, shown as the below windows:

```
Alarm Act Setting
on Main Moudle
```

```
Alarm Act Setting
on Door Moudle
```

```
Alarm Act Setting
on Extern Moudle
```

The first menu is “Alarm Act Setting on Main Module”. Press ENT to enter to the setting, LCD screen shows the current status of the alarm output. Y indicates the alarm output is enabled; N indicates the alarm output is disabled.

```
Alarm act on main
YN
```

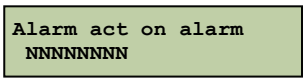
The main module provides two alarm outputs, press key “1” and “2” to toggle the alarm output 1, 2 ON and OFF

Press V to switch to “Alarm Act Setting on Door Module” submenu. Press ENT to enter to the setting, LCD screen shows the current status of the alarm relay outputs on the door module.

```
Alarm act on door
 NNNNNNNN
```

Up to 4 door modules can be installed on the NAV Controller. 2 alarm outputs are available on each door module. As a result, up to 8 alarm outputs can be available if 4 door modules are installed. Press numeric key 1~8 to toggle the alarm output on door module between ON and OFF.

Press V to switch to "Alarm Act Setting on Extern Module" submenu. Press ENT to enter to the setting, LCD screen shows the current status of the alarm outputs on alarm module.



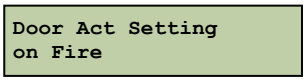
One alarm module can be installed on the NAV Controller. 8 alarm outputs are available on alarm module. Press numeric key 1~8 to toggle the alarm output on alarm module between ON and OFF.

Note the "Alarm Output on Alarm Module" is only shown when alarm module is installed on the controller.

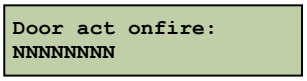
5.6.4.17 Door Act Setting On Fire

The controller allows the user to choose one of two behaviors to occur when a fire alarm is triggered: fail-safe or fail-secure. Door fail-safe at fire alarm means the door will be kept unlocked when there is a fire alarm input. Door fail-secure at fire alarm means the door will be locked when the fire alarm comes in.

In submenu list of "Alarm Input Setting", press ∧ and V to navigate to the below submenu to set the door behavior at fire alarm:



Press ENT to enter to the setting, LCD screen shows the current setting status of the door action when firm alarm is triggered.



In the menu shown above, press numeric key 1~8 to toggle the door action between fail-safe and fail-secure. (The numbers correspond to the number of door modules installed in the controller) "Y" indicates fail-safe; "N" indicates fail-secure.

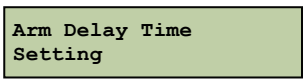
The default setting for door control at fire alarm is all the doors are fail-safe, *i.e.* all the doors will be unlocked during a fire alarm.

5.6.4.18 Arm Delay Time Setting

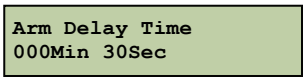
When an arm operation is executed, all active arm zones will enter ARM enabled status only after a certain time delay, which is called ARM delay time. When a card with ARM enabled is swiped to pass a door, system will not generate an alarm within the arm delay period so that cardholder has time to disarm the system.

The details to set ARM delay time is as following. And the alarm delay time can be set to different durations. In submenu list of "Alarm Input Setting", press ∧ and V to navigate to the below submenu to set the arm delay time:

Press ENT to set ARM delay time at the following window:



System will display the current delay time as shown below. Use numeric keys to input the desired ARM delay time. Enter minutes as a 3-digit number 0~999 and seconds as a 2-digit number 0~59. The default value of ARM delay time is 30 seconds.

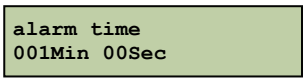


Press ENT to confirm. Press CLR to exit without effecting any change.

5.6.4.19 Alarm Out Time Setting

As described in alarm input mode, alarm timeout defines the duration of alarm output being presented (alarm relay energized), when triggered by the specified alarm input and if the alarm output mode is configured as “Latched” mode. After the alarm timeout duration, the alarm output will be reset to normal. The default alarm timeout duration is 60 seconds.

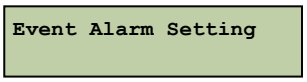
Note fire alarm has to be manually reset. It does not limited by the alarm timeout duration.



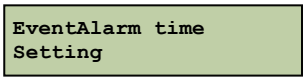
5.9.6 ALarm Event Setting

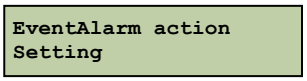
The physical alarm inputs can trigger alarm outputs. As described in previous section, the logic events, for example, unknown card, invalid card, expired card, invalid door and etc., can trigger the alarm outputs as well.

Press ENT at the below window to configure the event alarm setting.



Two submenus are included in event alarm setting: event alarm time setting and event alarm action setting, explained in the following sections. The screens of the two settings are shown below:





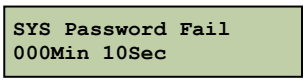
5.6.4.20 Event Alarm Time Setting

Press ENT at the screen of “Event Alarm Time Setting” to configure event alarm time setting. As introduced earlier, NAV Controller allows a logical event to trigger an alarm output. The duration of the alarm output can be specified per event type. Different event types can generate the different duration of the alarm output. The default value of event alarm time is 1 minute.

The following windows show the event alarm time setting on different events. All events will be explained one by one.

SYS PIN Fail

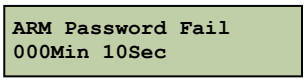
Please refer to section "Gain Access to System Configuration" in this chapter. A SYS PIN Fail event will be generated when user enters the PIN to enter system setting and a wrong PIN is entered three times consecutively. The time setting for system PIN failure event is shown in the below figure:



Press the numeric keys to input the specified alarm time for system password failure. Press ENT to confirm and press CLR to discard the change just made.

ARM PIN Fail

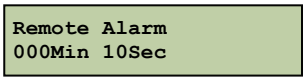
User is required to enter PIN when pressing ARM key to arm or disarm the system. An ARM PIN Fail event will be generated when a wrong PIN is entered three times consecutively. Please refer to the section "ARM/DISARM". The time setting for ARM PIN failure event is shown in the below figure:



Press numeric keys to input the specified alarm time for event of ARM PIN failure Press ENT to confirm and press CLR to discard the change just made.

Remote Alarm

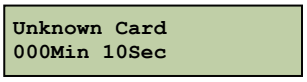
System administrator can directly generate alarm signal using the Control Software when he observes abnormal condition through surveillance system such as CCTV. This is defined as a Remote Alarm event. The time setting for remote alarm event is shown in the below figure:



Press numeric keys to input the specified alarm time for event of remote alarm. Press ENT to confirm and press CLR to discard the change just made.

Unknown Card

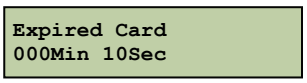
Unknown card refers to a card that hasn't been registered in the system. An Unknown Card event will be generated when an unknown card is swiped on the reader. The time setting for unknown card event is shown in the below figure:



Press numeric keys to input the specified alarm time for event of unknown card. Press ENT to confirm and press CLR to discard the change just made.

Expired Card

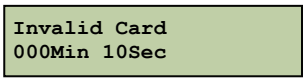
Any card in the system is usually assigned a valid date. After the valid date has passed, the controller will automatically set the card as an expired card. An expired card cannot gain access to the system. At the same time, an Expired Card event will be generated when an expired card is swiped on the reader. The time setting for expired card event is shown in the below figure:



Press numeric keys to input the specified alarm time for event of expired card. Press ENT to confirm and press CLR to discard the change just made.

Invalid Card

To disable a card, user can directly set the card as invalid card. An invalid card cannot gain access to the system. At the same time, an Invalid Card event will be generated when an invalid card is swiped on the reader. The time setting for invalid card event is shown in the below figure:



Press numeric keys to input the specified alarm time for event of Invalid Card. Press ENT to confirm and press CLR to discard the change just made.

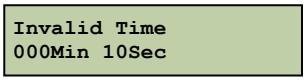
Invalid Door

Each door on the controller can be set its own access schedule, when a card is swiped on the reader. An Invalid Door event will be generated when a card is swiped at any door it can't gain access to system by the access schedule. The time setting for invalid door event is shown in the below figure:

Press numeric keys to input the specified alarm time for the event. Press ENT to confirm and press CLR to discard the change just made.

Invalid Time Section

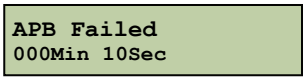
Each card belongs to an access group. Each group has its own allowed doors and time zones. That is, cards in the group have rights to pass which door at which time. An Invalid Time event will be generated when a card is swiped at any time it does not have right to pass. The time setting for invalid time event is shown in the below figure:



Press numeric keys to input the specified alarm time for the event. Press ENT to confirm and press CLR to discard the change just made.

Card Anti-Passback Fail

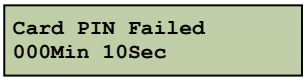
For more info on Anti-Passback, please refer to section Anti-Passback (APB) setting in this chapter. A Card Anti-Passback Fail event will be generated when the APB property of a card is set as enabled and that card is swiped twice consecutively on any enter-door reader or exit-door reader. The time setting for card APB fail event is shown in the below figure:



Press numeric keys to input the specified alarm time for the event. Press ENT to confirm and press CLR to discard the change just made.

Card PIN Fail

For password setting, please refer to section “Set Card PIN Setting” in this chapter. A Card PIN Fail event will be generated when the card is swiped at the reader and PIN is required to gain access but the cardholder enters wrong PIN three times consecutively. The time setting for card PIN fail event is shown in the below figure:



Press numeric keys to input the specified alarm time for the event. Press ENT to confirm and press CLR to discard the change just made.

Door Forced Open

A Door Forced Open event will be generated when controller detects that a door is opened from the door sensor without any legitimate swipe card or door open button push operation taking place. The time setting for door forced open event is shown in the below figure:

Press numeric keys to input the specified alarm time for the event. Press ENT to confirm and press CLR to discard the change just made.

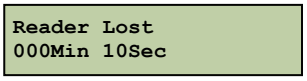
Door Held Open

A Door Held Open event will be generated when a door is opened by legitimate swipe card or door open button push operation but is still not closed after the “over time” in door setting has elapsed. The time setting for door held open event is shown in the below figure:

Press numeric keys to input the specified alarm time for the event. Press ENT to confirm and press CLR to discard the change just made.

Reader Lost

A Reader Lost event will be generated when controller detects that the reader has no signal. The time setting for reader lost event is shown in the below figure:



Press numeric keys to input the specified alarm time for the event. Press ENT to confirm and press CLR to discard the change just made.

Panic Open

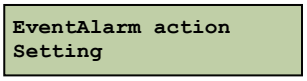
Panic Open alarms are designed to allow users who are forced to enter a building under duress to silently trigger an alarm. When the door's access schedule is configured as PIN needed, for example: "Card or PIN" or "Card plus PIN", cardholders can type in their panic PIN to trigger a panic open event in the system.

The panic PIN is the cardholder's original PIN plus any two digits. For example, Sam's PIN is 12345678. He can type in any two more digits following"12345678" as the panic PIN, such as "1234567800".The time setting for panic open event is shown in the below figure:

Press numeric keys to input the specified alarm time for the event. Press ENT to confirm and press CLR to discard the change just made.

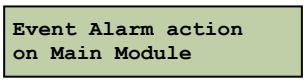
5.6.4.21 Event Alarm Action Setting

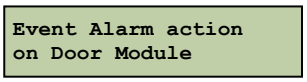
Press ENT at the below screen to configure event alarm action setting.

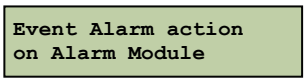


The event alarm action defines which alarm output can be triggered by the event. As we explained before, NAV Controller can take main modules, up to 4 door modules and 1 alarm module, total 18 alarm output. Users will be able to configure the event to trigger any one or multiple outputs from those 18 alarm outputs.

The event alarm action setting includes three submenus, shown in below.







The alarm output setting on these three screens are the similar. For example, the fire alarm event actions on door module will look like:

The top line indicates the event to be configured. The bottom line is the setting of alarm outputs on 4 door modules. Y indicates there is alarm output (relay energized) and N indicates there is no alarm output (relay not energized). R refers specifically to alarm output on the door module, indicating that alarm output will be generated only if the event occurs on the corresponding door. The above example means the alarm output relay at door 1 will be energized if door forced open event happens on any door, the alarm output relay at door 2 does not respond to any door forced open event, and same as door 4 to 8. Door 3 indicates the alarm output relay on door 3 will be energized if and only if the door 3 got a forced open event.

Note "R" option for alarm output does not apply to alarm module and main module, since they don't naturally correspond to a door control.

In the above menu, press numeric key 1~8 to toggle the alarm output actions of this event on the door module among Y, N, and R (only for door module). Press ∧ and ∨ to navigate to other alarm action settings.

The default setting of all the event alarm actions on main module, door module and alarm modules are all disabled. The event alarm actions for main module and door modules are listed below. Default settings for event alarm actions on alarm module are same as door module, not listed here.

Main module	Door module
SYS Password Fail NN	SYS Password Fail NNNNNNN
ARM Password Fail NN	ARM Password Fail NNNNNNN
Remote Alarm NN	Remote Alarm NNNNNNN
Unknown Card NN	Unknown Card NNNNNNN
Expired Card NN	Expired Card NNNNNNN
Inavid Card NN	Invalid Card NNNNNNN
Invalid Door NN	Invalid Door NNNNNNN
Invalid Time NN	Invalid Time NNNNNNN
APB Failed NN	APB Failed NNNNNNN
Card PIN Failed NN	Card PIN Failed NNNNNNN
Door Forced Open NN	Door Forced Open NNNNNNN
Door Held Open NN	Door Held Open NNNNNNN
Reader Lost NN	Reader Lost NNNNNNN
Panic Open NN	Panic Open NNNNNNN

5.10 Network Setting

Correct network settings are needed for NAV Controller to get online and be accessible remotely. Network setting includes DHCP setting, IP address setting.

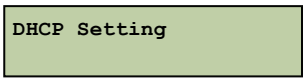
Press V five times from main menu items to view the below screen:

```
Network Setting
```

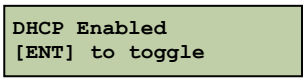
In the above screen, press ENT to enter the network setting submenus.

5.10.1 DHCP Setting

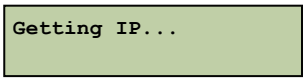
DHCP setting is the first submenu under network setting. Press ENT from the below screen to configure DHCP setting.



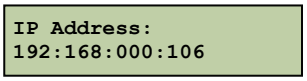
The below screen will be shown in the DHCP setting submenu. Press ENT key to toggle between DHCP (DHCP enabled) and static IP (DHCP disabled). The default DHCP setting is disabled by default.



When DHCP is enabled, press CLR to exit and NAV Controller will update the IP address from DHCP server and show the below screen, indicating the controller is getting IP address:



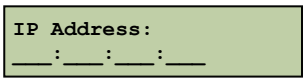
After the IP address has been obtained, controller shows the IP address in the below window:



At this window, press ENT to update the IP address again. Press CLR to exit to “DHCP Setting” window.

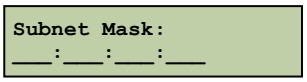
5.10.2 Set IP Address

For a static IP setting, users need to manually set an IP address. Press ENT under the below submenu of Network Setting to set IP address:

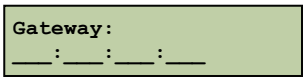


Input the desired IP address and press ENT to confirm. The default IP address is 192.168.1.200

When using static IP (DHCP disabled), NAV Controller will require the subnet mask and gateway setting automatically after the IP address is set here.



Input the desired subnet mask and press ENT to confirm.

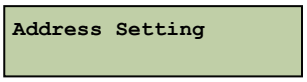


Input the desired gateway IP address and press ENT to confirm.

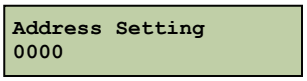
5.11 Address Setting

NAV Controller is connected to network for remote accessibility by IP Address, but it must have a unique address for the purpose of communications and control by the Management Software when there is more than one controller.

Press V six times from main menu items to view the below screen:



Press ENT to enter to the address setting menu, as shown below:

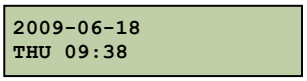


5.12 Arm/Disarm

After an alarm module is installed, it defines 10 arm zones for its 10 alarm inputs (including the 2 alarm inputs on main module). NAV Controller can treat alarm inputs in 10 arm zones in a very flexible manner. These 10 arm zones can be armed or disarmed on the controller as described below.

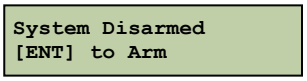
5.12.1 Arm the Systemusing the Controller Keypad

User must have the ARM PIN in order to utilize this function. Please refer to the section “Set ARM PIN” in this chapter for instructions on how to set ARM PIN. After system installation, the date and time information will be displayed on the LCD, as shown below:

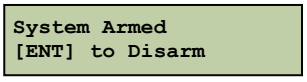


When ARM on the keypad is pressed, the system prompts the user to enter a password, as shown below:

After entering the password, press ENT to confirm. The default password is 00000000. Once the password is verified, the current system ARM status will be displayed as shown below:



Press ENT to arm all active arm zones. The following message is displayed:



Press CLR to exit. The controller will wait for the period of time defined as “alarm delay” and then arm all active arm zones.

5.12.2 Disarm the Systemusing the Controller Keypad

In order to utilize this function, the user must have the ARM PIN and the card must be logged in as ARM enabled. Assuming the system is in armed status, the user swipes the card to access the door. The controller will disarm all active arm zones in arm delay time. For example, if the system is in armed status and a card is presented, the controller will disarm all active arm zones for the amount of time

assigned as the arm delay. During this time, no alarm outputs will be generated even if an alarm input is triggered.

Similar to the procedure to arm the system, press ARM on the keypad. Input the ARM password and press ENT to confirm. After the password is verified the current system ARM status will be displayed as shown below:

```
System Armed
[ENT] to Disarm
```

Press ENT to disarm all active arm zones. The following message is displayed:

```
System Disarmed
[ENT] to Arm
```

Press CLR to exit.

5.12.3 Reset Alarm

When system is generating an active, ongoing alarm output, follow the procedure below to reset the alarm.

At the window showing the system time, press ARM on the keypad. Input the ARM password and press ENT to confirm. After password is verified the following menu window appears:

```
Reset Alarm?
[ENT] to Reset
```

Press ENT to clear the alarm. If system is currently armed user will be prompted to disarm the system first. Please refer to previous section for how to disarm the system.

5.12.4 Arm/Disarm the Systemusing aKeypad Reader

The whole system can also be armed and disarmed using a keypad reader. (The reader must have an integrated keypad, and the keypad and system reader settings must be enabled on the controller in order to utilize this feature. Please refer to subsection “Reader Setting” for instructions on enabling these features.) The part number for the EverAccess keypad reader is ERK-871.

The user must first enter a command to get into the arm operation mode. (The command is introduced in step 1 below.) In the arm operation mode, the yellow LED on the ERK-871 will show the four different system modes outlined below:

Yellow LED Status	System ARM Status
OFF	Indicates that the system is disarmed
ON	Indicates that the system is armed
Flashing Slowly	Indicates that the system is in arm delay period
Flashing Quickly	Indicates that the system is armed and some alarm input has triggered the alarm output.

The steps to arm or disarm the system at a keypad reader are as followed:

1. Press“*” key on the keypad and input 8 digits ARM password, then press “#” key to arm/disarm the system.
2. If the system is in disarmed mode (the yellow LED is OFF), press“#” to arm the system. The system will enter the arm delay period (the yellow LED will slowly flash).

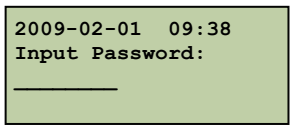
   If the system is in armed mode (the yellow LED is ON) or in the arm delay period (the yellow LED is flashing slowly), press “#” to disarm the system. Then the system will enter the disarmed mode (the yellow LED will be off).
3. In any system mode, press “*” to exit the arm operation. If no key is pressed for 20 seconds, the reader will automatically log out of the arm operation mode.

5.12.5 Arm/Disarm the Systemusing aLCDReader

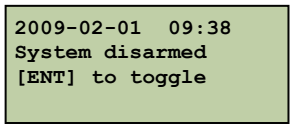
New model of readers, ERL-871 in EverAccess series was released to provide a more intuitive user interface to interact with the system. ERL-871 provides a large LCD to show more information from controller.

The steps to arm/disarm system with ERL-871 are explained below:

1. Press “*” on keypad, input 8 digits ARM password and press “#” to confirm.



2. After entered the ARM menu, press “#” key to arm/disarm the system. Press “*” to exit the system.



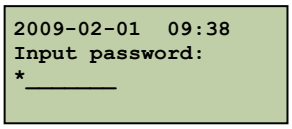
5.13 Use Reader as Keypad

Access control system provides a keypad to control a door and approve or deny an access request. NAV Controller provides the same function with the correct setting.

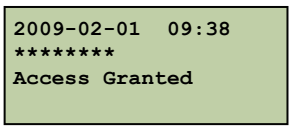
To use PIN only to access a door, set the door verification mode as “Card or PIN or fingerprint”, and set the keypad reader with the enabled keypad property. When these setting are all configured right, users can key in the valid card PIN at the keypad reader and press # to gain the access. If the PIN matches the records in the system and the door verification mode allows, the controller will unlock the door.

Take the operation on ERL871 LCD keypad reader as example, the steps to use PIN only to access are listed below:

1. Press any numeric key on ERL871 keypad, the below screen will show and the first inputted key will be stored there already:



2. Press “#” key to confirm the inputted PIN. If the PIN is verified OK, the below screen will be shown. If PIN retry failed 3 times, system will show “ERR” on screen and return to the main page of ERL871.



Chapter 6

6. Software Introduction

6.1 Main Feature

EverAccess® NAV Controller not only can do basic setting configurations on it, but also can login through the browser (Here and later referred to as “Software”) for system setting configurations. NAV Controller can manage EverAccess Flex I/II/Fingerprint series controller, and also store and maintain the system data. It provides the basic attendance function based on the stored data. In the browser, the user can configure EverAccess CCTV products, to achieve access control and monitor linkage function.

The Software interface contains clearly defined functional modules. Windows-based structure design facilitates effective management. The main interface provides an over view of operation options and graphical toolbar allows a more intuitive operation.

The Software offers different levels of operation authority to prevent unauthorized access. User name and password is required to login to the Software. The system database is encrypted. User setting is designed to distinguish users with different operation authorities. Users belonging to different authority groups have different operating privileges in the Software. In addition, endures PIN access and multi-card access enhances the efficacy as well as the security of the access control system.

6.2 Hightlight Performance Overview

- Manage different Series Controllers
  - Support ELA890, Flex I, Flex II Access controllers.
- Supports accessory Hardware
  - Support Desktop reader, USB card reader, fingerprint scanner etc.
- Support multiple operating system platforms
  - Compatible with Windows2000 operating system or higher.
- Good user interface design, easy to operate
  - Vista-style user interface
  - New icon design
- Database Management
  - Support for FTP, the local database backup, restore function

- Supports Multiple Language Mode
  - Support Chinese, English, Russian
- Software Features
  - Real-time monitoring of controllers, doors, arm zones, alarm input/output and fire alarm on electrical maps, allowing operators to directly monitor system status and responds accordingly.
  - Support remote control of controllers, doors, arm zones and alarms.
  - Support endures PIN access and multi-card access.
  - Size of operating windows and panels can be adjusted.
  - Simple and practical attendance management.

6.3 Baseon TCP/IP Access Conttrol System Architecture

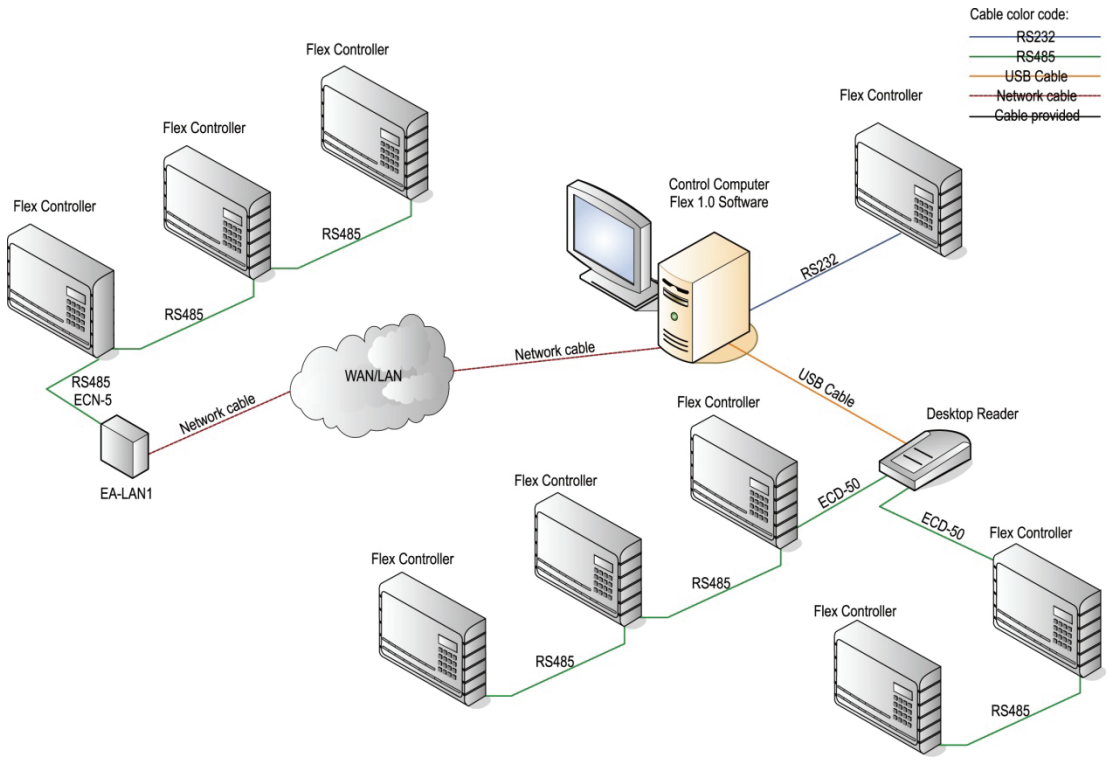


Figure0-1System Architecture Diagram

Chapter 7

7.Start to Use

This chapter introduces how to quickly setting EverAccess® NAV Controller as a super administrator and use the controller to control doors and collect attendance records and CCTV linkage function through browser. Please follow the steps to get familiar with the software. For a more comprehensive understanding of each function, refer chapters on related topics.

7.1 Quick Start

7.1.1 Add and Configure Controller

In the main interface, click “Access Control” ➔ “Controller” ➔ “Controller Setting” enter to controller setting page. The steps to add a controller shown as following (the detail refers to 12.1.1).

Steps：

1) Click the “Add” button, input controller mode number, location and address.
2) Click the “Save” button.

Set Access Rule

7.1.2.1 Set Date

Click on the menu bar “Access Control” ➔ “Access Rule” ➔ “Date Type”, enter to date type page. Below is how to add a date type (Detail setting see 13.1.1)

Steps：

1) Select recurrent type.
2) Select the date in calendar.
3) Select date type
4) Input the date remark.
5) Click the “Save” button.

7.1.2.2 Set door schedule

Please set door schedule before distribute different schedules to each door. Click on the menu bar "Access Control" ➔ "Access Rule"➔ "Door Schedule", enter to the door schedule setting page. Below is how to set a door schedule (Detail setting sees 13.4.1).

Steps：

1) Click the "Add" button.
2) Input the name of new schedule in the text box.
3) Click modify schedule, in the pop-up dialog box to set time and the door area authentication, save and then close the dialog box.
4) Click "Save" and save the completed plan.

7.1.2.3 Set Access Door

Click on the menu bar "Access Control" ➔ "Access Rule" ➔ "Access Door", enter Access Door Setting page. (Detail please sees 13.5)

Steps：

1) Select a door schedule for each door location of controller.
2) Completed setting of door schedule for each door, click the "Save" button and system will prompt a pop-up window "modified successfully".
3) Click the "Confirm" to finish the setting for Door Access.

7.1.2.4 Set Group Schedule

Click on the menu bar "Access Control" ➔ "Access Rule"➔ "Group Schedule", enter Group Schedule Setting page. Bellow is how to add a group schedule (Detail setting please sees 13.2.1).

Steps：

1) In the "Schedule Name" text box, input the new schedule name.
2) Click the time period under the "Day setting", pop-up dialog box where the user can modify the schedule and entry mode.
3) After modify schedules, click the "Save" button and the new schedule will be added to the access group schedule list.

7.1.2.5 Set access group

Click on the menu bar "Access Control" ➔ "Access Rule"➔ "Access Group", enter Access Group Setting page. Bellow is how to add an access group (Detail please sees 13.3.1).

Steps：

1) In the access group text box, input the name of new group.
2) Select different door location of different controller, lock level and door access schedule.
3) After completed all the setting of each controller, click the "Save" button.

7.1.3 A Varietyof WaystoAdd Cards

Software provides a variety ways to add the card to the system. Users can choose any way to achieve this functionality. The follow describes how to add a separate card and the allocation of the corresponding control groups.

Access group's default is "Full Granted"; default password is "000000". First select the card format users want to add.

7.1.3.1Quick add card

When the user has logged in software, swipes card on the controller, then swiped card recording shown in the system event log, this time can through copying. (Detail sees 7.3.5.1).

Steps：

1) Add new card through the reader.
2) Log in software, in the system event records (Records of Normal card access and illegal card access); it will show card number, copy the card number.
3) Select the correct card format.
4) Go to "Cardholder" page to add a new card. Click "Save".

7.1.3.2 Card Setting Interface

Click on the menu bar "Access Control" ➔ "Card" ➔ "Card Setting", enter to cards setting. Below is how to add a card and the allocation of access groups. (Detail sees 14.2.1).

Steps：

1) In "Card Type Setting" page, select the card format.
2) Click the "Add" button and enter to the Card Setting Page.
3) Fill out all properties of card.
4) If a cardholder name has been added, the card can be assigned to the cardholder.
5) Select an access group for the card.
6) Select card private schedule. When the card applies the private schedule, it will follow private schedule to verify enter and exit.
7) Click the "save" button and setting completed.

7.1.3.3 Import Cards Using Excel File

In Excel, edit the card data (no quantitative restrictions), save as CSV file to import the card through software features to complete the registration card to the controller (whether registered to the controller of this card depends on the access group setting, if there is no choice access group options, they are given the default access group "Full Granted").

Click on the menu bar "Access Control" ➔ "Card"➔"Import Card"

Steps：

1) Click the "Browse" button, select the Excel file to be imported, click the "Next".

2) Select the relevant column name corresponds to the value.
3) Click “Import” button and add completed.

7.1.4 Setup Departemnt and Cardholder

7.1.4.1 Set Department

Click on the menu bar “System” ➔ “Cardholder”➔ “Department Setting”, enter to Department Setting page. Here’s how to add a new department (Detail sees 9.1.1 Add department).

Steps：
1) Click the “Add” button.
2) Fill out department name
3) Select the parent department
4) Click “save” and setting completed.

7.1.4.2 Add Card Holder

Click on the menu bar “System” ➔ “Cardholder”➔ “Cardholder Setting”, enter to Cardholder Setting page. Here’s how to add a cardholder (Detail sees 9.2.1).

Step：
1) Click the “Add” button, pop-up a page to add cardholder.
2) Fill out employee number, name, department, and other information, upload photos.
3) Here can add a new card to the cardholder.
4) Click “Save” button and completed.

7.1.5 Configuration and Attendance

7.1.5.1 Set Attendance Time

Click on the menu bar “Attendance” ➔ “Basic Setting”. Select a menu for different attendance day type. Bellow is how to edit a day type (Detail setting please sees 16.1).

Steps：
1) Select a day type menu, enter to the page.
2) Select a department and edit.
3) Click the “Save” button.

7.1.5.2 No-Access-Attendance

Click on the menu bar “Attendance” ➔ “Attendance Exception” ➔ “No-Access-Attendance”. Below is how to add a no-access-attendance enrollment for a cardholder (Detail please sees 17.1.1).

Steps：

1) Click the “Add” button.
2) Select a cardholder form the list, select the time and other information.
3) Click the “Save” button.

7.1.5.3 Time-off Enroll

Click on the menu bar “Attendance” ➔ “Attendance Exception” ➔ “Time-off Enroll”, enter to time-off page. Here’s how to add a time-off enrollment for a cardholder (Detail setting please sees 17.2.1)

Steps：

1) Click the “Add” button.
2) Select a cardholder form the list, select the time and other information.
3) Click the “Save” button.

7.1.5.4 Overtime Enroll

Click on the menu bar “Attendance” ➔ “Attendance Exception” ➔ “Overtime Enroll”, enter to Overtime page. Here’s how to add an overtime enrollment for a cardholder (Detail please sees 17.3.1).

Steps：

1) Click the “Add” button.
2) Select a cardholder form the list, select the time and other information.
3) Click the “Save” button.

7.1.6 Real-time Monitoring

Click on the menu bar “System” ➔ “Real-time monitoring” ➔ “Real-time Event”, enter to the Real-time Event page. The upper page displays current the real-time status of the electronic map. User can select different map in the map list on the left hand side of the page.

On the bottom page, it displays current real-time status. User can click to check the detail.

7.1.7 Export Function

Most of the system function modules are provided “Export” feature on the page, click the “Export” button, pop-up dialog box to save the document, the page information in CSV format for export, shown as following：

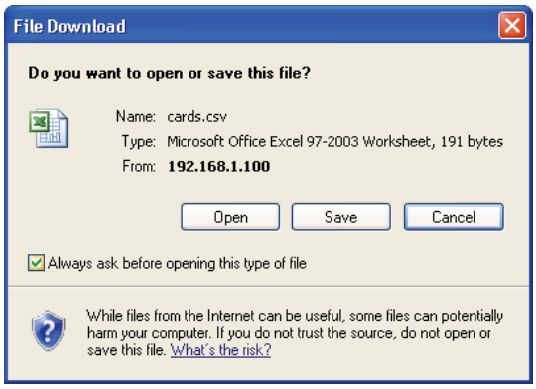

File Download
Do you want to open or save this file?
Name: cards.csv
Type: Microsoft Office Excel 97-2003 Worksheet, 191 bytes
From: 192.168.1.100
Open
Save
Cancel
Always ask before opening this type of file
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

Figure7-1Export

Click the "Save" button; select a path to save the exported document, shown as following:

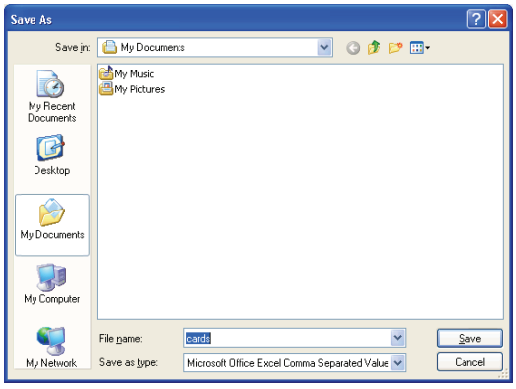


Figure7-2Save

Select the path and click "Save" button, export CSV format file to complete.

! Note: If the excel file contains Chinese, you need to convert the file, if open the file directly, the Chinese characters are garbled display. Each file conversions of the import/export function in the system please refer to the following method, and it will not repeat.

Steps:

1) Right-click the saved CSV file, select "Edit" in the drop-down menu.
2) The system default, use Notepad to open the file, click "file" in the menu bar and click "Save As", shown as following:

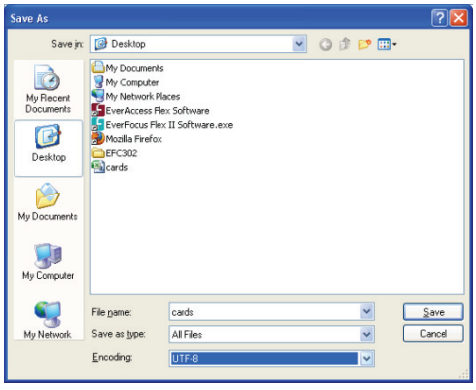


Figure 7-3 Convert the Exported File

3) In the dialog box, select Save as type "All Files", select encoding "UTF-8".

4) Click the “Save” button, the conversion is completed.
5) Open the converted file via Excel, the Chinese displays properly.

7.1.8 Print Function

Most of the system function modules are provided “Print” feature on the page, click the “Print” button, enter to the printing page (Figure 7-4). The system on the operation of printing features are the same, will not repeat

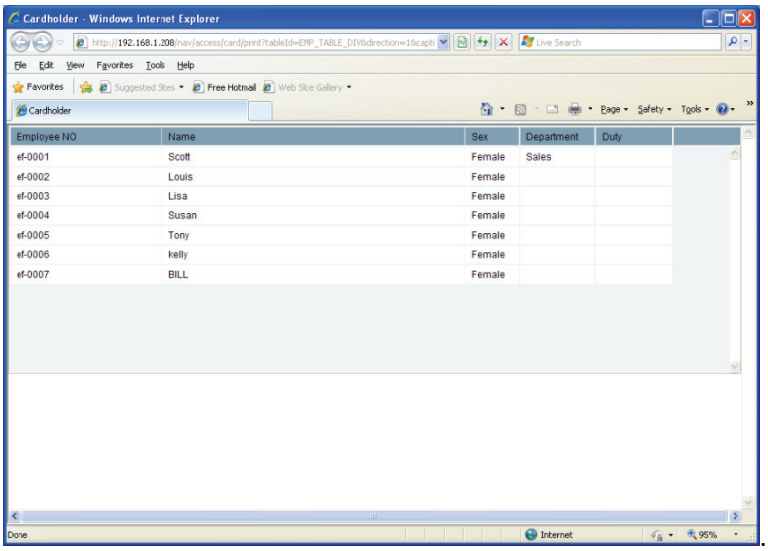


Figure7-5Print Users’ Information

7.2 Login

Open a browser and type IP address in the address bar, if setting of controller is still factory setting, the default controller IP address is 192.168.1.200. According to the page you are prompted, input the login name, password and verification code, and then click “Login” button, shown in Figure 7-6:

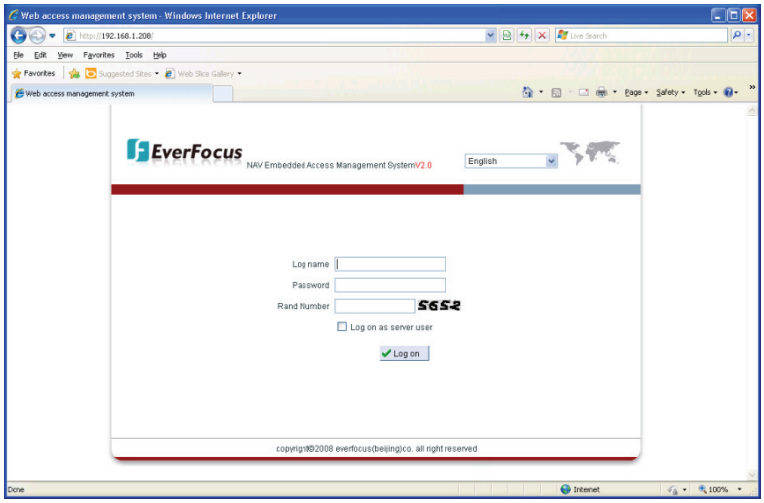


Figure 7-7Login Page

Upper right corner of the page can choose to the language, NAV Controller support Chinese, English and Russian.

The default login setting shown as following:
User Name: admin
Password: admin

Note: admin is a special “super administrator”, it is used for system installation and recovery setup for main purpose, its possession all the rights does not change. The user cannot be deleted and just only change the password. Please login first to make amendment and remember the passwords in order to ensure the security.

Modify the super administrator password through the menu “System” ➔ “Basic Setting” ➔ “Change Password” to change the password. Super Administrator through the menu “Basic Setting”➔ “User Setting” ➔ “Add” to create users and change the new user’s group. If other users have been removed, also the super-administrator’s password is lost, will not be able to login the software.

In the login page, enter a user name and password, choose whether “central server user login” and then click “Login” button, enter to the NAV Controller’s browser page.

If the user name or password inputs in error, it will prompt pop up “illegally logged”, shown as following

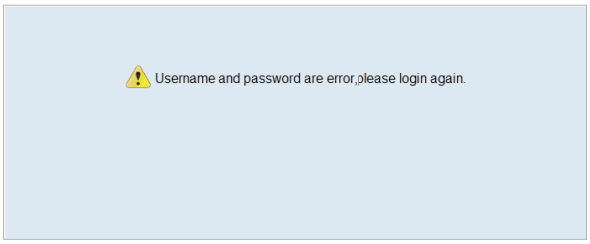


Figure7-8Illegal Login

7.3 Familiar with the Browser Page

7.3.1 Main Page Introduction

Using humanized design concept to ensure that users get started. Enter to the home page. Please see as following:

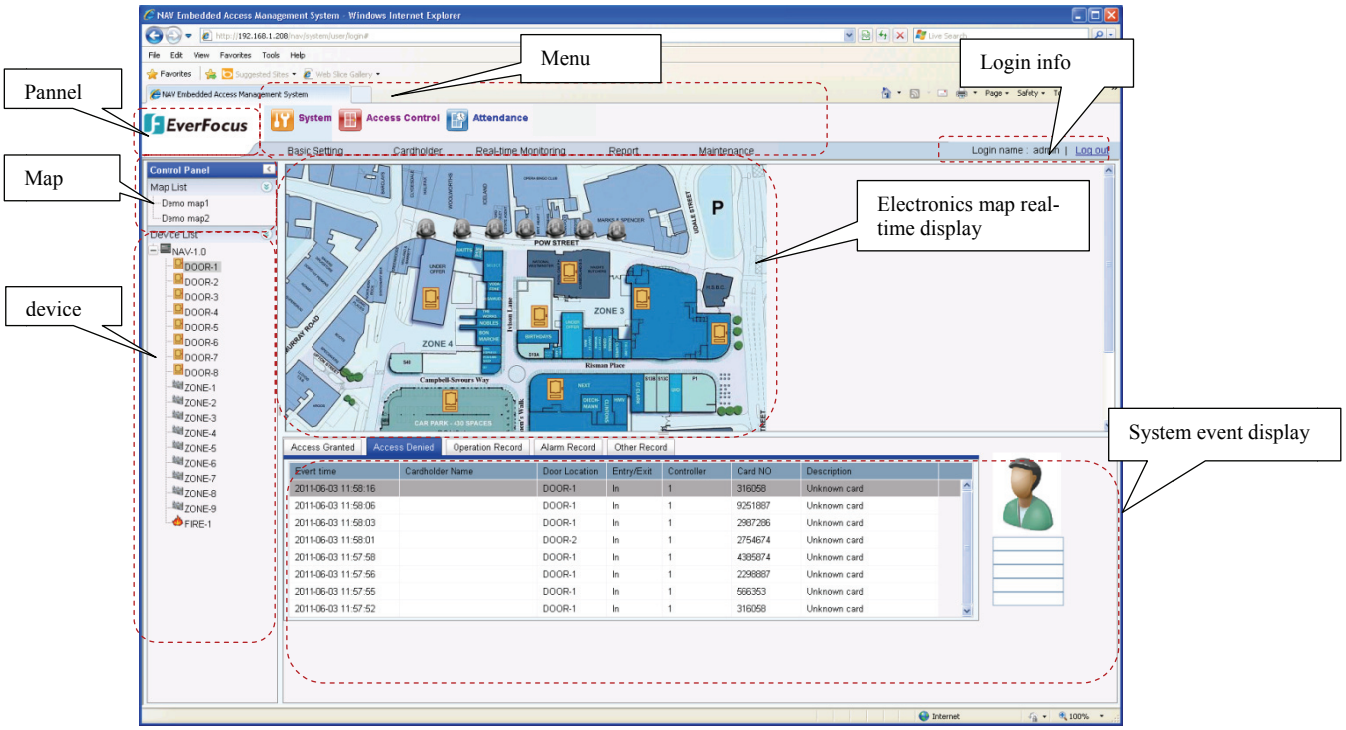


Figure 7-9Main Page

7.3.2 Menus

There are 4 main menus in the software, including System, Access Control, Attendance and CCTV (Figure7-11). Click on each main menu will show its sub-menu options. Click on each sub-menu will open a corresponding function, the specific features in later chapter for detail.

Figure7-10Menu

If the logged-on user does not have access to a module function, then the feature does not appear in the menu bar.

7.3.3 Control Pannel

Click the “Control Panel” and “Device List” are hidden (Figure 7-9). When the user click the button area or double-click the hidden area, it will show the control panel and device list on the main interface.

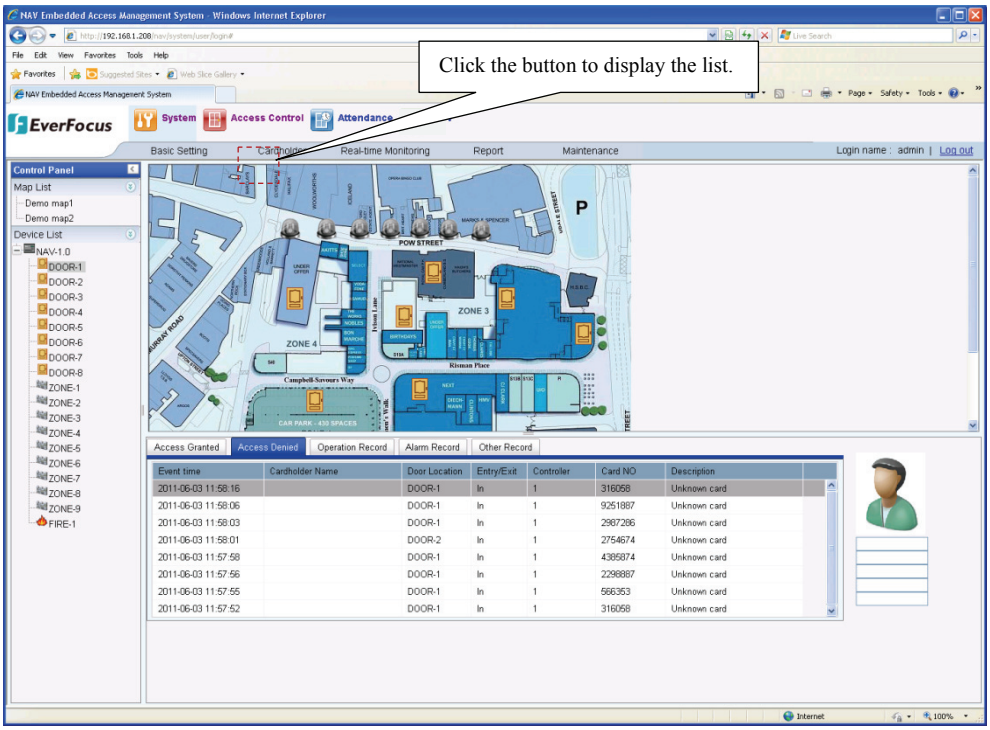


Figure 7-11Hide the Left Side of Control Panel

7.3.3.1 Electronic Map list

This area shows the complete setting of electronic map structure in the software (Figure 7-10). Please refer to 10.2 for detail of adding, deleting and revising of electronic map.

Figure 7-12Electronic Map

7.3.3.2 Device List

This area displays effective devices which have been configured by the software (Figure 7-11). If controller have been added or deleted or revised, it will be showed in this area.

Figure 7-13Device List

7.3.4 Real-time Monitoring

This feature displays real-time electronic map status, the user can click on “Electronic list” to switch different electronics maps and keep track system state. For more detail about adding, revising and deleting of electronic map, please refer to 10.2)

7.3.5 System Event Record

This area displays system in the region records of all incidents, including access granted, access denied, operation record, alarm record, other record. There is a bar on the top of the record panel, use this bar to adjust the size of the panel.

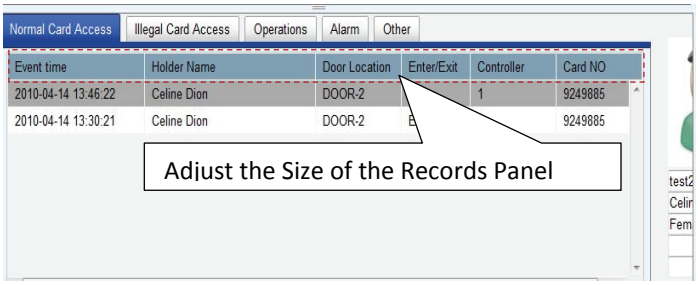


Figure 7-14 Adjust the Size of Panel

7.3.5.1 Access Granted

This type is including: normal access record, access by card’s password and access by APB Violation.

Each record is including: event time, cardholder, door location, entry/exit, controller and card number. Select one record, the cardholder information will be shown on right hand side panel.

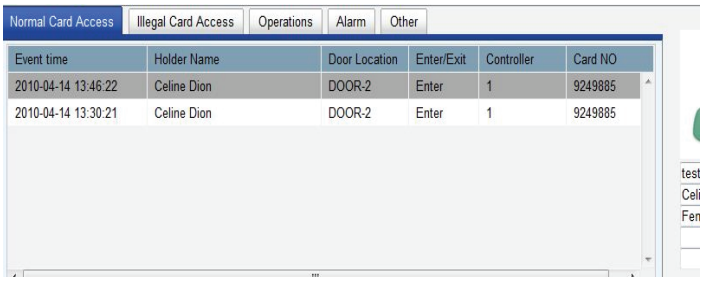


Figure 7-15 Access Granted

7.3.5.2 Access Denied

This type is including: Unknown card, Expired card, Invalid card, Password retry failed, Enter with panic PIN, Insufficient multi-card access, Invalid time,. Invalid door, APB fails, No PIN inputted, Man trap violation, Access denied due to unknown card PIN.

Each record is including: event time, cardholder, door location, entry/exit, controller, card number and description.

Figure7-16 Access Denied

7.3.5.3 Operation Record

User remote control, Armed/disarm, reset alarm, press button open, interlock etc.

Operation control record is including: event time, location, controller and event.

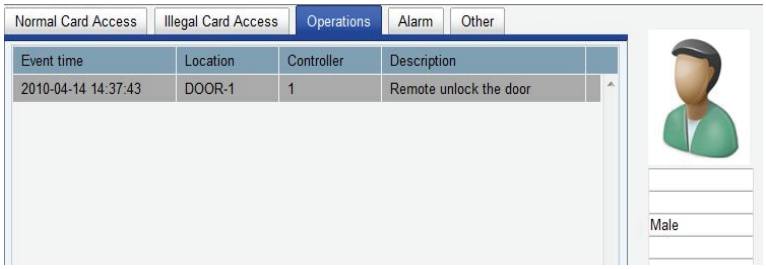


Figure 7-17 Operation Record

7.3.5.4 Alarm Record

The type include: zone alarm, fire alarm, system password error, zone password error, tamper alarm, remote alarm, forced open door, panic open door, open door overtime and reader lose

Alarm event record is including: event time, location, controller and event.

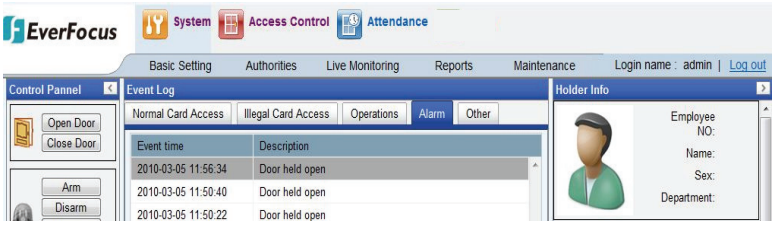


Figure 7-18Alarm Record

7.3.5.5 Other Record

In the system, other records which related to the controller setting, including: event loss, power-down, add reader, controller on line, controller off line and controller power-up.

System setting record is including: event time, location, controller and event.

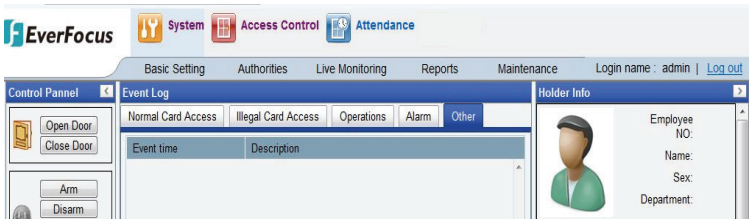


Figure 7-19Other Record

Chapter 8

8. Basic Setting

This chapter will introduce basic setting of EverAccess® NAV Controller. It is including change password, user groups setting, user setting, local server configuration, system upgrade and center server configuration.

Change Password: revise login password.

User Groups setting: add, delete and modify the software and permission groups. No limit on their number, the user can add permissions groups as needed.

User setting: add, delete and modify the users operate the software. The default administrator is admin. It has all operating privileges, only modify the password of super administrator.

Local sever configuration： Configure IP type, address, gateway, date, time and so on.

System Update: upgrade online and upgrade local.

Center server configuration: center server configuration refers to the “ENS2000 NAV series WEB Network Access Control Management software” (not the built-in software) address and password configuration etc. The configured controller can be used as a sub-station to be connected and managed to the ENS2000 software.

8.1 Change Password

Here Password is for the current user logging to NAV Controller built-in browser software, it just only modify its login password.

First of all, the user must input the old password, then enter and repeat the new password. Click the “Save” button to save. If the input is wrong, user can use the “Reset” button to refill.

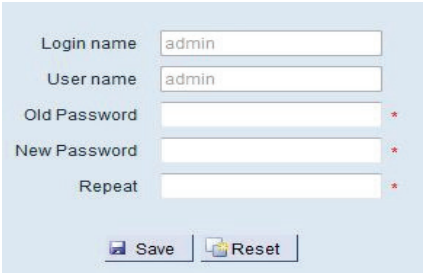


Figure 8-1Change Password

8.2 Set User Group and User

In this system, a user means a person to operate the software, because of permissions used for different pages will be different. Each user is defined by the four kinds of attributes: name, login name, password, user group.

“Name” means user’s real name. “Login Name” is the user login to the system is required to type identity. “Password” is the system login is required to type a password. “User Group” will introduce in the following.

Note: The “user” and “Cardholder” are different. Cardholder is the person accesses the control systems (such as the company’s normal staff). User is the person through operating software to monitor or configure the access control system.

The users in the same group operate the software restricted level. Different group have different restriction on the software operation.

Click on the menu bar “System” ➔ “Basic setting” ➔ “User Group”, enter to user group setting page. User groups setting please see 8.3.

First enter to the “User Groups” page. The system has three initial groups.

Default 3 kinds of groups are system administrator, manager, common user. There is no user limit for each group.

System administrator: Users can use all features of this software system, including: basic management, personnel management, access control, attendance management, database management etc.

Manager： Users can use all features of this software system except basic setting.

Common user： Users can use all features of this software system except basic setting and database management.

The following table lists the specific function of each group; “√” indicates that the functions are available in the group.

Function		system administrator	manager	common user
System	Change Password	√	√	√
	User Groups setting	√		
	User Setting	√		
	Local Server	√	√	
	System Update	√		
	Center Server	√		
	Department Setting	√	√	
	Cardholder Setting	√	√	
	Import Cardholder	√	√	
	Real-time Event	√	√	√
	Edit Electronic Map	√	√	
	Cardholder Report	√	√	√
	Data Backup	√	√	

	Data Recovery	√	√	
	Purge Out-of-date Data	√	√	
Access	Controller Setting	√	√	
	Data Download to the Controller	√	√	
	Date Type Setting	√	√	
	Access Door Setting	√	√	
	Door Schedule Setting	√	√	

	Access Group Setting	√	√	
	Group Schedule Setting	√	√	
	Card Type Setting	√	√	
	Card Setting	√	√	
	Import Card	√	√	√
	Card Report	√	√	√
	Card-dependent Event	√	√	√
	Card-independent Event	√	√	√
Attendance	Working Day	√	√	
	Weekend	√	√	
	Special Day	√	√	
	No-Access-Attendance	√	√	
	Time-off Enroll	√	√	
	Overtime Enroll	√	√	
	Original Access Record	√	√	√
	Report By Cardholder	√	√	√
	Statistics by Cardholder	√	√	√
	Statistics by Department	√	√	
CCTV	DVR Setting	√	√	√
	View Setting	√	√	√
	Multi-View Setting	√	√	√
	Linkage Monitoring	√	√	√

Figure8-1Feature List of Each Group

The group "system administrator" cannot be edited or deleted. The other two group groups can be edited or deleted.

8.3 User Group

User groups setting page, on the left shows the current user group list (Figure 8-2). If the user has the authority to set the user group setting, then can create, modify, and delete any group.

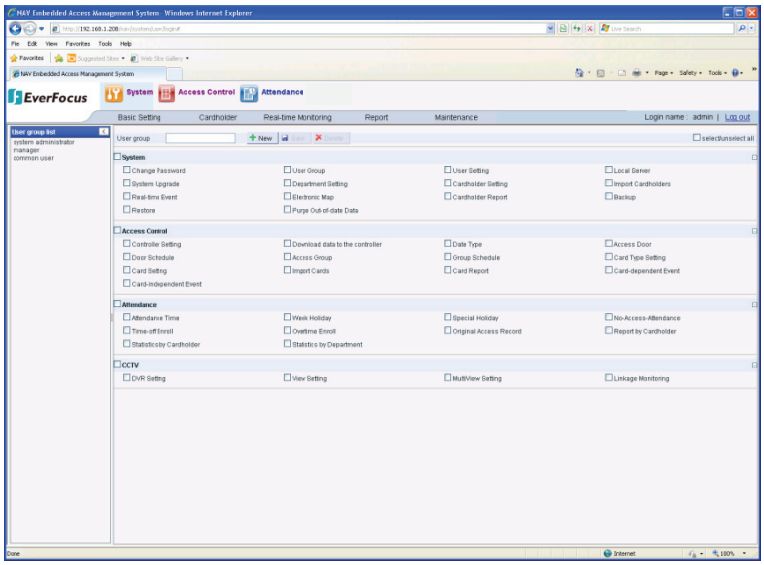


Figure 8-2User Groups

8.3.1 Add A Group

Click the “New” button on the top of the setting page. Input the new group name in the “Group Name” box. Check the operation detail of the user group’s authority, editing is completed, click the “Save” button.

8.3.2 Edit A Group

Select a user group to modify on the left hand side of the setting page. The user can edit the authority group name and operation details. After edit finished, click the “Save” button.

8.3.3 Delete A Group

Users can select the permissions group to delete on the permission group list. Click the “delete” button, system will ask confirm the delete (Figure 8-4). After click “OK”, Deletion is completed.

NOTE: A user group using by users cannot be deleted.

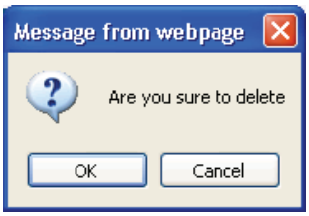


Figure 8-3 Confirm to Delete a Group

8.4 User Setting

Users setting means create, modify and delete users, specify the user group. The user is actually talking about here refers to the software can log on and use the account, and different from the employee. User is including login name, password, user group, user names and other information. Default super-user is “admin”, and belongs to “system administrator”. Super-user cannot be deleted.

Click the menu “System” ➔ “Basic Setting” ➔ “User Setting”, enter to the users setting, shown as following:

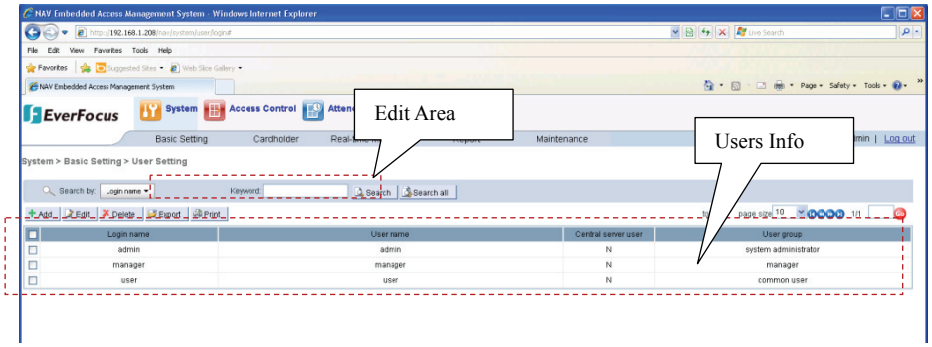


Figure8-4User Setting

8.4.1 Add A User

Click on “Add” button, pop-up Add User page (Figure 8-6). Enter login name, user name, and password. Select the group name, click the “Save” button, a new user is added to the user list.

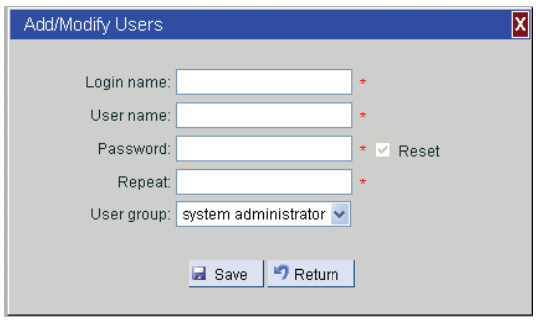


Figure8-5Add a User

Login name: the name for user login and use the software that can be made by numbers, letters, spaces, Chinese characters and characters can be displayed any combination of up to a maximum 20-bits, every character counts 1 bit. Login name are case-sensitive letters. It cannot be same as the existing ones and not be empty. If the user enters one already existed, the system will be prompted.

User name: user real name, it is used to facilitate system management, must be filled.

Password: can be numbers, letters, spaces, Chinese characters and other characters can be displays any combination of up to 20-bits, every character counts to1 bit. The letter is case-sensitive password.

Repeat: password must be entered with the same content, if two-times input are inconsistent will be prompted “Input the password do not match”.

User group: the group that the user belongs. The user can be assigned a new user to any group, system administer group can operate all functional module.

8.4.2 EditA User

Select a user to be modified, click the “Edit” button, pop-up Edit user box (Figure 8-7). The user’s login name, user name, password, and user groups can be modified. If user wants to reset the user’s login password, check the “reset” button and edit. After edit finished, click the “Save” button, the system returns “Operation successfully” box. If no changes to make, click “Cancel” button to return to the “users setting” page.

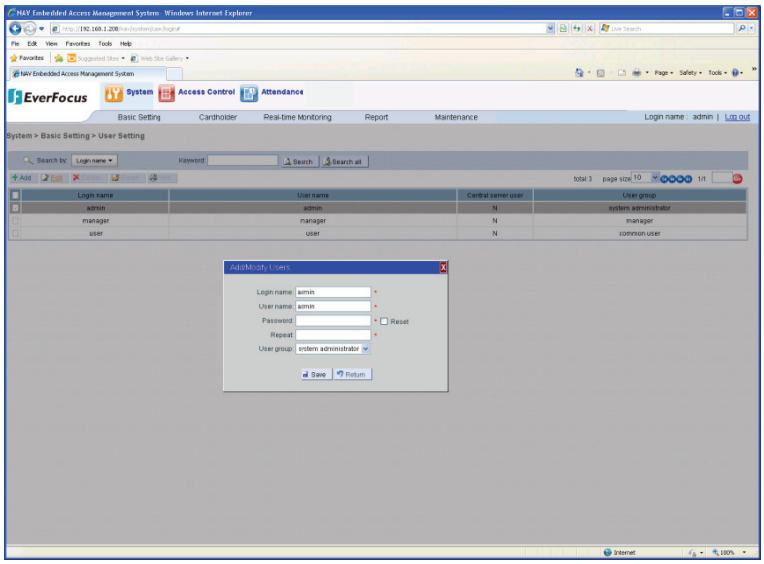


Figure8-6Edit a User

8.4.3 Delete A User

Select a user to be deleted, click the “Delete” button, the system will pop-up a box to confirm “Are you sure to delete?”, click “OK” means delete, delete operation is complete.

Note: The default user “admin” cannot be deleted.

8.4.4 Export Users

Click the “Export” button, system will pop-up a save box, all users’ information in order to export the CSV format, select the path to save the document, click “OK” to confirm. Please refer to 7.1.7 for detail.

8.4.5 Print Users

Click the “Print” button, enter to the printed page. Please refer to 7.1.8 for detail.

8.4.6 Search Users

Type the conditions of the corresponding content into the search box, and click the “Search” button, such as system has meet the requirements of information will be displayed in the bottom of the list (Figure 8-8). When the search is completed, click “All” to go back to the users setting page.

Note: “Search” means precise queries.

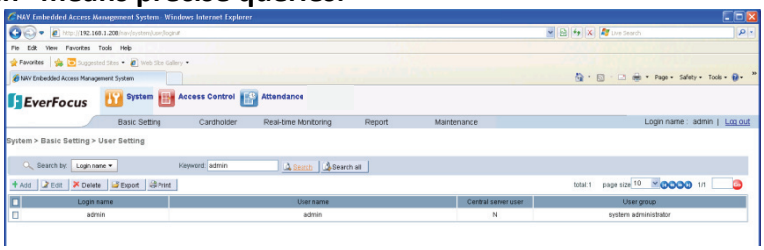


Figure 8-7Search Users

8.5 Local Server

The local server configuration can be set to the controller currently logged IP, time, date and time zone.

In system main menu, click “System” →“Basic Setting”→“Local Server”, shown as following:

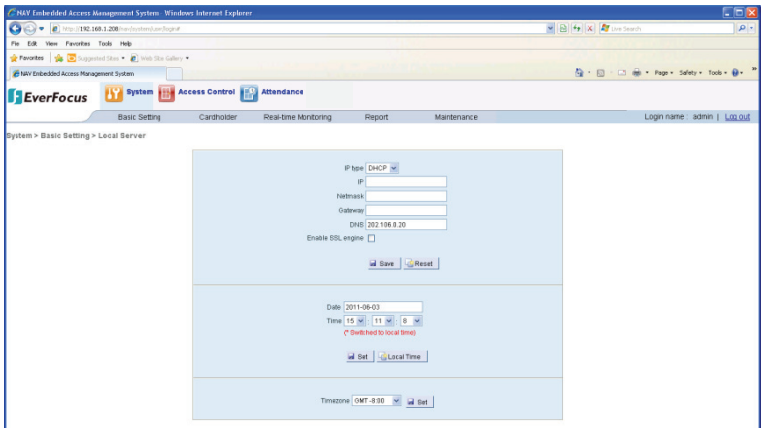
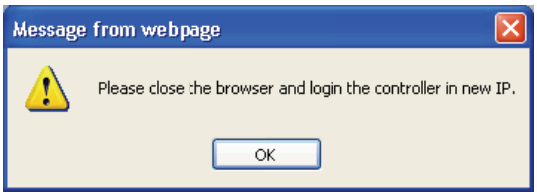


Figure8-8Local Server

Select the static or dynamic IP type, input the IP, subnet mask and gateway, click the “Save” button, as below picture.



Continue to click “OK”, according to the revised IP address to log back controller.

Click “Reset” button will display the network setting on the page input box.

Click “Local time” button and make controller time and local time synchronization. Users can also set up the time as needed. Click “Set” button to save users’ time setting.

Choose time zone, click the “Set” button to complete the time zone setting.

8.6 System Upgrade

The firmware of controller and built-in software can be upgraded to the latest version as the user needs by the operation. There are two ways including remote on-line system update and local update.

Click system main menu “System” →“Basic Setting” →“System Upgrade”, enter to the system upgrade page, as following (Figure 8-10), the default entry is online upgrade page.

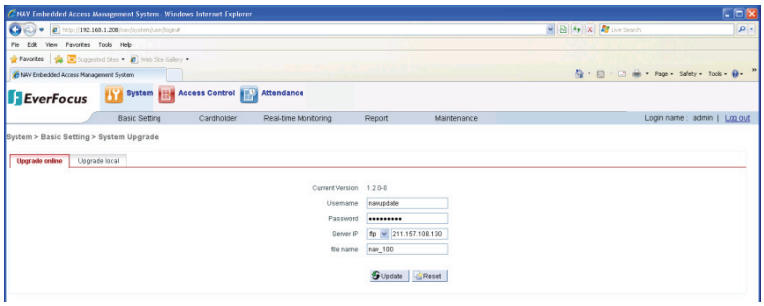


Figure8-9Online Upgrade

8.6.1 Upgrade Online

Upgrade by inputting the IP address and account of remote FTP or HTTP server and account. Input the accurate address and account number. Click the “Update” button. After finished, please log in again.

8.6.2 Upgrade Local

Using the upgrade package provided by the service to do local upgrade. Click the “Browse” button, select the package, and click the “upload” button. After completed, please log in again.

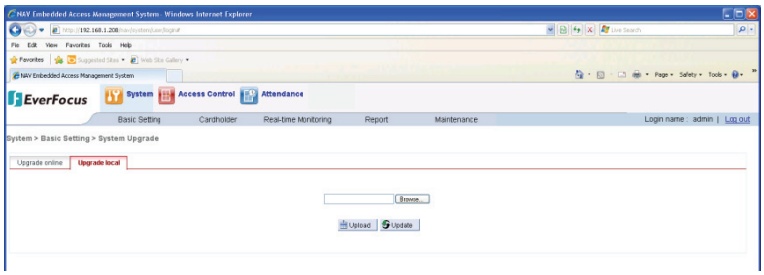


Figure8-10Local Upgrade

Chapter 9

9. Cardholder

This chapter introduces EverAccess® NAV Controller's cardholder management, including: department setting, cardholder setting and import cardholder.

Department setting: Set the department information.

Cardholder setting: Set employee number, full name, department and other basic information, and employees can be assigned one or more cards, set its properties etc.

Import cardholder: the edited CSV (Excel) format file to import into the controller.

9.1 Department Setting

Click on the menu bar "System" ➔ "Cardholder" ➔ "Department Setting", enter to the department setting page, shown as following:

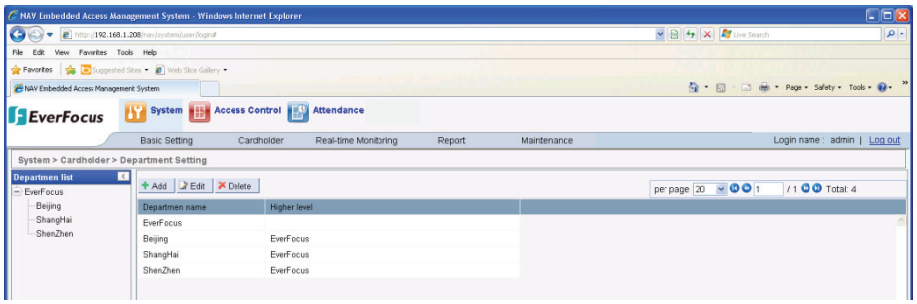


Figure9-1Department Setting

The left side panel is a tree showing the company's organizational structure (all departments). On the right side of page show all the child departments of the selected node in the tree. User can add, modify and delete a department on the right side. After completed, system will automatically save.

Set the department' detail information. Organizational structure is divided into three layers, the first layer is company, the second layer is department and the third layer is group.

9.1.1 Add A Department

Click "Add" button, system will pop-up a window, shown as following:

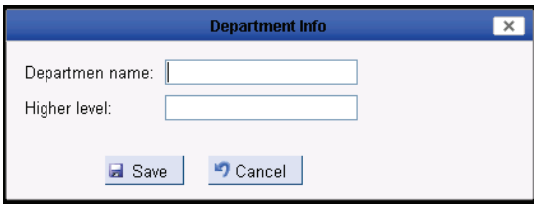


Figure9-2Add a Department

Input the department name, click the “High level” input box to select the parent department. Save and back to department setting page.

Department names cannot be repeated if they are in the same level and it is suggestion that not use existing name in the other level for the new one.

9.1.2 Edit A Department

Select a department and click “Edit” and modify department information，see Figure 9-3:

Figure9-3Edit a Department

Enter department name in the input box, click the department which is parent of current edit department, and through modify the parent department to change current edit department’s level. Click “Save” and return to the department setting page.

9.1.3 Delete A Department

Select the department that need to be delete, and click “Delete”，see Figure 9-4：

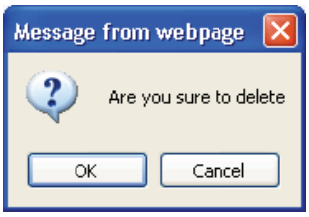


Figure9-4Confirm to Delete a Department

Click the “OK” button, it will be deleted and its corresponding node will be deleted from the tree.

Note: Cannot delete a department with lower level departments, shown as following:

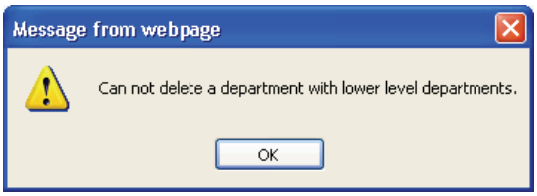


Figure9-5 A Department with Lower Level Departments cannot be Deleted

9.2 Cardholder Setting

Click on the menu bar “System” ➔ “Basic setting” ➔ “Cardholder” ➔ “Cardholder Basic Information”, enter to the cardholder information page, shown as following:

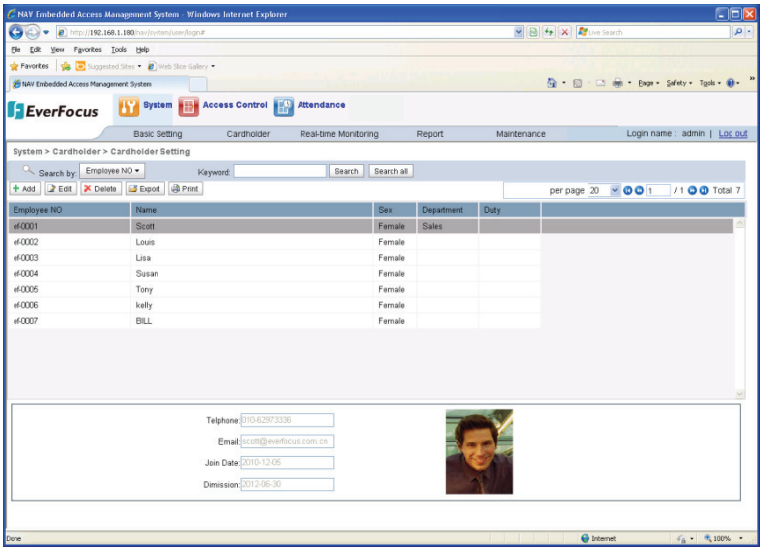


Figure9-6 Cardholder Setting

The upper of the page is query area, the middle is operating area and the lower is the detail.

At the top right side of the operating area, users can set the quantity of cardholders per page. The system default value is 20 records. In addition, flip button, jump button will help users quickly reach the page they want. Please see Figure 9-7

Figure9-7 Operation Area

9.2.1 Add ACardholder

Click the “Add” button, system pop-up new cardholder’s detail page, shown as following:

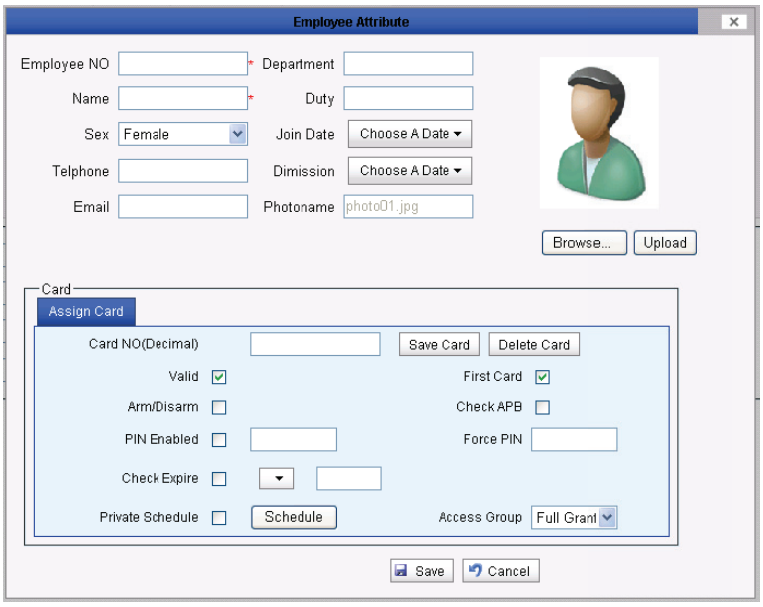


Figure9-8Add a Cardholder

1) Cardholder Information Area: This area is setting cardholder's basic information.

Employee number: can be any printable character, it is a unique number for a cardholder. If new member joined, the new number cannot be same as existing number. System will prompt "Fail to save the employee".

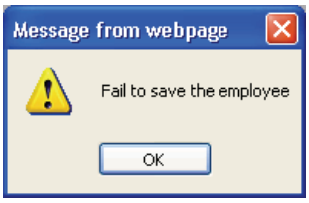


Figure9-9Fail to save the employee

Name: cardholder's real name.

Sex: the system default setting is "Male".

Department: click to choose the department that new employee will belong to.

Join/Demission date: when click the input box, will pop-up the calendar box. Choose the date.

Figure 9-10Pop-up the Calendar Box

Photo: Click the “Browse” button, pop-up the window to choose the uploading photo, select one and click the “Upload” button to upload to the system.

Steps:

1) Select a picture upload: Click the “Browse” button, locate the photo to be uploaded, make sure the size must be not more than 2M.
2) Upload files: After a photo is selected, click the “Upload file” button.
3) Photo name: When the photo has been uploaded, the file name will be listed there.

! Note: Employee number and name is required, the other is not, but it is suggestion that the user completed the detail in order to query more intuitive display of information.

2) Card information area： This region is assigning one or more cards for the employee, and set the relevant properties of the cards.

The area is associating current employees with the cards. Input the associated cards’ serial number (a string of number or symbols printed on the most cards), or connect ERU Series USB desktop reader (see ERU series hardware manual) and fill the card serial number by swiping card automatically.

Card format: There are three card formats in the system, decimal, hexadecimal and NNN-NNNN. Users need to choose the correct card format before adding the card in the menu “Access Control”→“Cards”→“Card type”.

Add a Card: Input the serial number and click the “Save Card” button, it will be saved. A cardholder can assign one or more cards. If the number is same as existing one in the system, it will prompt “The card was been assigned to others, modify it?” shown as following:

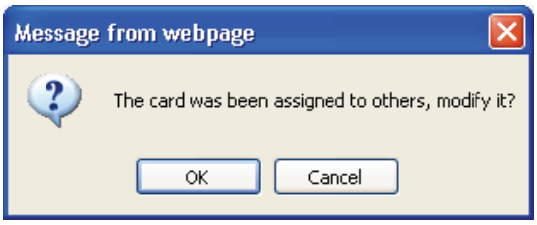


Figure 9-11Assigned to other cardholder’s Card

Delete an assigned Card: Select one first, click the “Remove Card” button, the card will be removed.

Note: This operation is real-time processing.

All the properties of a card are showing as following, check the check box of the item to enable and uncheck to disable:

Card valid: whether the registered card is valid. Check the check box to enable the card. The other card properties will work only if the card is enabled. Swiping a card that is not registered with the controller generates an “unknown card” record. Swiping a card that is registered but disabled generates an “invalid card” record.

First Card: whether the card is a “first-card” that can trigger unlock in door setting (refer to door setting) and “first-card-in” function in controller setting (refer to system setting). For

example, suppose door 1 under controller 0001 is set to “unlock” in time zone 9:00-11:00. During this time period, swiping a first-card enabled card unlocks the door. In addition, if “first-card-in” function is enabled for controller 0001, only after a first-card enabled card has been presented to a reader under controller 0001, will other first-card disabled cards be able to unlock the door, even though those first-card disabled cards satisfy all other conditions to unlock the door

Arm valid: whether the cardholder has the right to arm/disarm the system on a keypad reader. When an arm enabled card is presented to the reader, the system will be disarmed for a time period so that the cardholder can enter/exit the arm zone without triggering an alarm. This time period is defined by arm delay time in the system.

APB Valid: whether anti-passback (APB) is enabled for the card. If APB_EN is enabled for a card, and the controller APB function is enabled, the APB setting is in effect for the card. Refer to Anti-Passback (APB) setting for details

Password status: Cardholder can set up an 8-digit door password for NAV Controller. To enable/disable, use functions in door setting, access authority setting or card schedule setting.

Note: if need to use password feature, the reader must to be a keypad reader.

Panic Pin: it is used when the cardholder was under duress and only work when the door zone is set to password required. It is 2-digit numbers. When uses Panic pin, input the normal first 6-digit password, and then input 2-digit panic pin. Alarm will occur when it confirm, also door open.

Expire date: whether the card has an expiration date. If Card Expiration is checked, the card can only be used within the expiration date. An expired card cannot gain access to the system and an “expired card” event will be generated if an expired card is swiped on a reader. The time set in the expiration date is the end of the expiration date. It can be accurate to minute.

Card Schedule: refers to the verification mode for cardholders to enter/exit doors. Card schedule setting is shared with access group schedule setting. To select a special card schedule for a card, user needs to add a new schedule in “access group schedule setting” and then apply the schedule for the card in “card schedule”. If "card schedule" is enabled, the system will follow the card schedule. In this situation, door verification control will not be applied to this card.

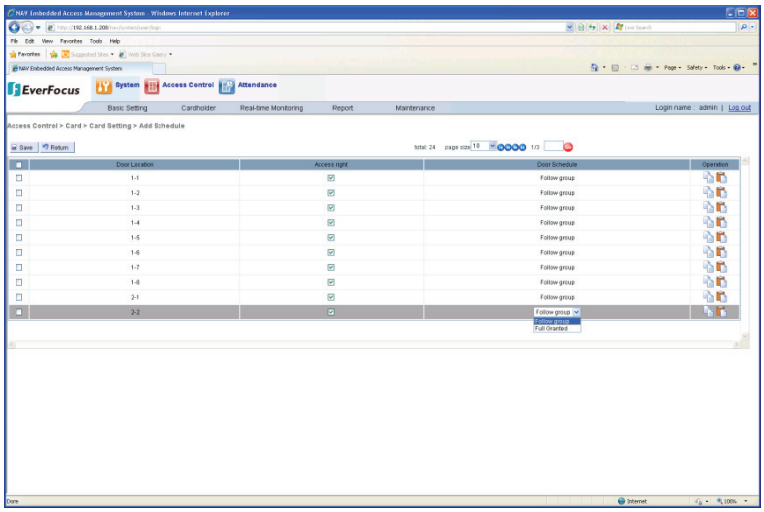


Figure9-12Card Schedule Setting

Select different access schedule for different door zone. Different access schedule will specify the card which has one kind entry rule for each door zone.

Note: All cards in one group can be assigned to different access group in different controller.

When finished all the detail information of the card, click on “OK”, the operation is completed.

Access Group: The card can be assigned to 2048 kinds of access groups, different groups will be set a different access rules.

9.2.2 EditA Cardholder

Select a cardholder in the cardholder list to be edited, click the “Edit” button. Enter to the cardholder edit page, shown as following.

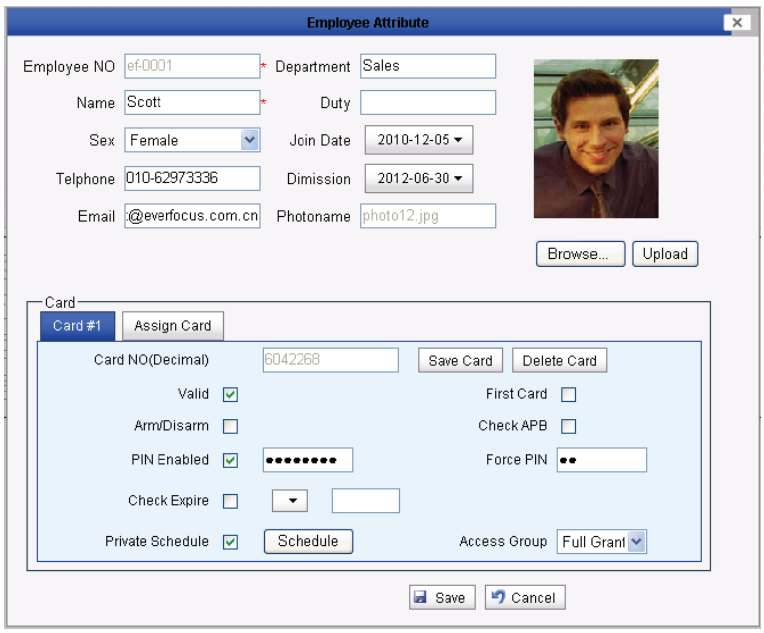


Figure 9-13Edit a Cardholder

Edit a cardholder's information is similar to adding a cardholder. After edition is complete, click the "Save" button to save the change.

9.2.3 Delete A Cardholder

Select a cardholder in the cardholder list to be deleted, click the "Delete" button, op-up as below:

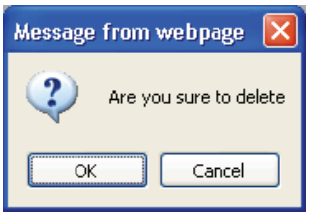


Figure 9-14Confirm to Delete a Cardholder

Click the "OK" button to confirm.

Press on the keyboard "Shift" key to select the cardholders to be deleted, click the "Delete" button to confirm if delete all the selected cardholders. Click the "OK" button to delete all the selected.

9.2.4 Export CardHolders

Click the "Export" button, pop-up download file box, all cardholders will be exported to CSV format, select a path to save the file. Click "OK" to confirm. Please see 7.1.7 Export function.

9.2.5 PrintCardHolders

Click the "Print" button to enter to the printing page, the specific operation method see 7.1.8 Print function

9.2.6 Search CardHolders

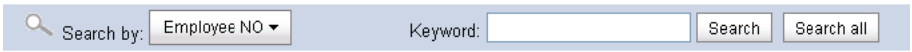


Figure9-15 Search Cardholders

Select a search field and input the search criteria in the "keyword" text box, click the "Search" button to start searching. If there are cardholders matching, they will be shown in the cardholder list. Click "Search All" button, back to the all cardholder list.

9.3 ImportCardholders

Select System menu bar "System"→ "Cardholder" → "Import Cardholders", and then enter to import page, shown as following:

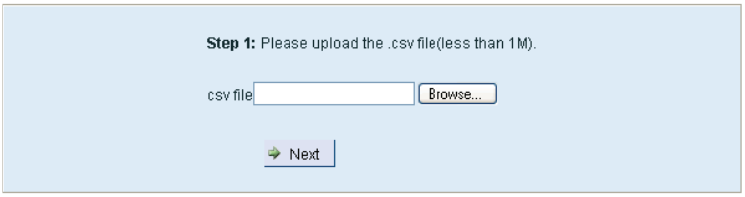


Figure9-16 Update Excel File

Steps:

1) Upload Excel format file, click the “Browse” button, and locate the file want to upload. Imported file must be CSV format (Excel 97-2003), and less than 1M.
2) Click the “Next” button to enter to the operation page, shown as following:

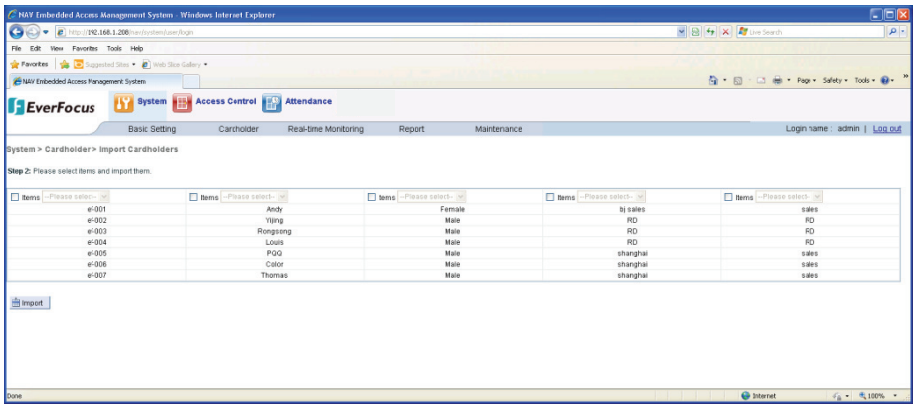


Figure9-17Import Cardholders

3) Click the drop-down menu of attributes, and select the corresponding attribute categories, and check the attribute box on the top of column.
4) Click on “Import”, system starts to import the cardholders.
5) Displayed after the completion of “xxx records have been imported.”
6) Click “Back” button, go back the import cardholders page.

Note: All data imported to the system must be in CVS format, select the path to import the document, click OK to finish.

Chapter 10

10. Real-time Monitoring

10.1 Real-time Event

Click on system menu bar “System” → “Live Monitoring” → “Live Events”, and enter to the Real-time events page; see figure below:

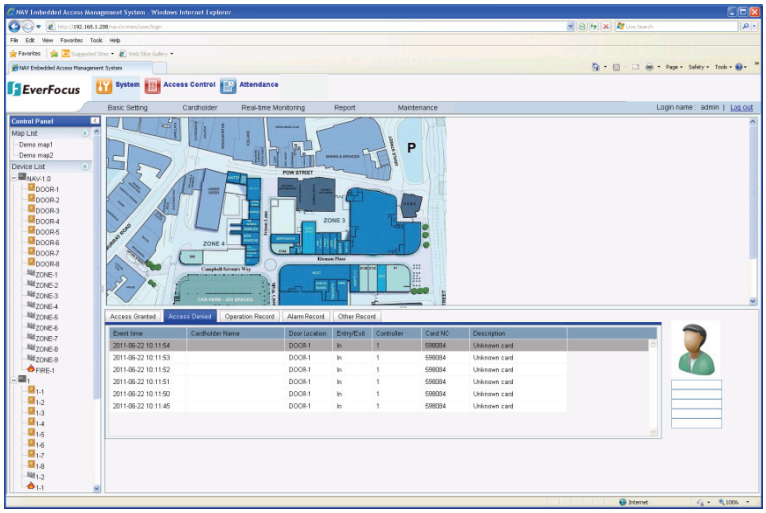


Figure10-1Live Event

As shown in the above figure, the real-time event monitoring page is divided into three basic areas.

Map list and device list located on the left side, it shown all the map list, controllers and doors, arm zones, DVR, CAM and View. The users can easily remote control open/close, set alarm etc.

Electronic map is located in the top of the middle. Each device’s real-time status is displayed by its icon. Such as door is opened or closed, control is armed or disarmed etc.

The real-time event records are located in the bottom of page. They are listed in order of receiving automatically listing each now event at the top allowing for scrolling and displaying in real time.

Cardholder information of each record is positioned in the right bottom corner of the page, which is used to display the cardholder detail. When each different real-time event is received, this section will display each cardholder’s detail, such as cardholder’s photo, name, gender, department etc. If the record is not related to the cardholder, the related contents in this column will be blank.

! Note: substation only caches some real-time event records. When the user enters the real-time event record page at the first time, it only displays some real-time event record of the station. If the user inquires the old records, needs to go to card access inquiry page to search.

10.1.1 Remote Controller

Click the node in map list and device list and a menu will pop-up containing remote operations, such as arm, disarm, reset alarm and add map etc. Clicking on the door node will show the menu to select between “Open Door” and “Close Door”.

10.1.2 Remote Dvr and View

Click the node in the resource tree contains DVR, CAM or View. According to the type of node, it will pop up corresponding functional menu. Click the node will preview and can be added to the electronic map.

10.2 Edit Electronic Map

Click on the menu bar “System” → “Real-time Monitoring” → “Electronic Map”, enter to the Electronics Map edit page, shown as following:

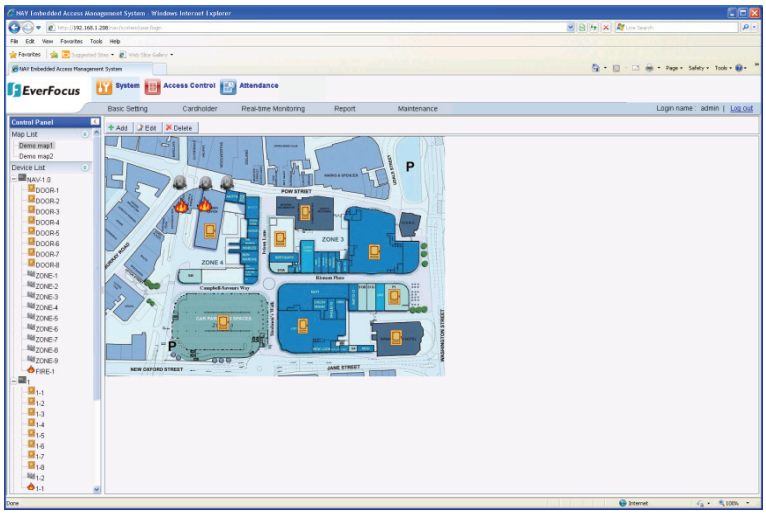


Figure10-2Edit Electronic Map

10.2.1 Add An Electronic Map

Click the “Add” button, pop-up following window:

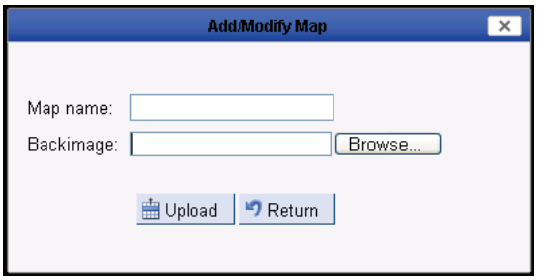


Figure10-3Add an Electronic Map

Map name: name for a new electronic map.

Back Image: click the “Back Image” button, to pop-up a page to add a local map. Then click the “upload” button and upload the map to the server. Click the “Back” button to get back to the main page.

10.2.2 Edit An Electronic Map

Select the map image by a single click and click “Edit” button, enter to the edit page. See figure below:

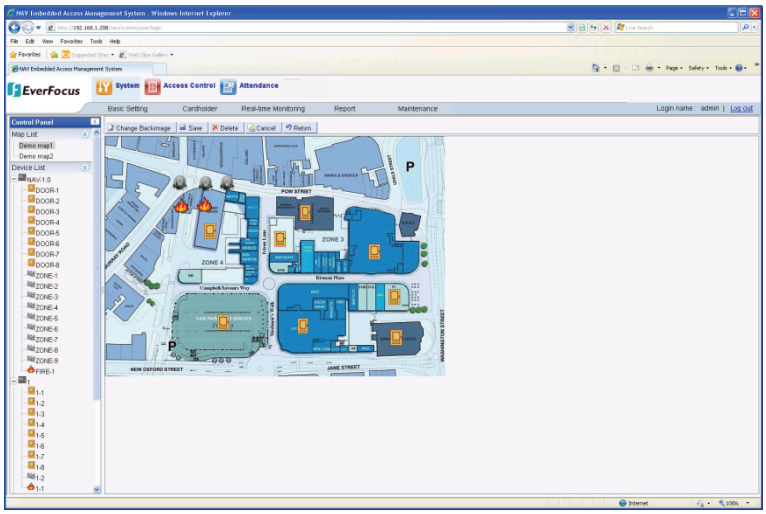


Figure10-4 Edit an Electronic Map

There are 5 operating buttons in the edit area: back image, save, delete, cancel and return. See figure below:

Figure 10-5 Operating Button

5.6.4.22 10.2.2.1 Back Image Setting

Click the “Back Image” button, and the following box will pop-up:

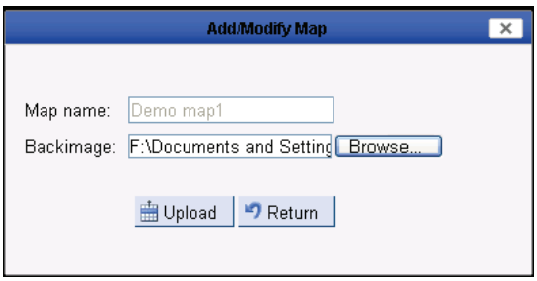


Figure10-6Back Image Setting

Click “Browse” button to select an image and upload to the server.

5.6.4.23 Add Device Icon

Click the node in the device tree on the left side of main page, the device icon will show on the left side corner in electronic map, use the mouse to move or drag and drop the device to the desired place on the map, Click the “Save” button to save.

Save: Save the electronic map.
Delete: Delete the current electronic map edited.
Cancel: Cancel the operations on the electronic map.
Return: Back to main page.

10.2.3 Delete An Electronic Map

Select the map which need to delete on the map list, click the “delete” button, a pop-up a confirm box will appear saying “are you sure to delete”, click “Ok” to confirm, otherwise cancel the delete feature.

10.3 Report

10.3.1 Search Cardholders

Click on system menu “System” → “Reports” → “Cardholder”, the system enters employee information query page, see figure below:

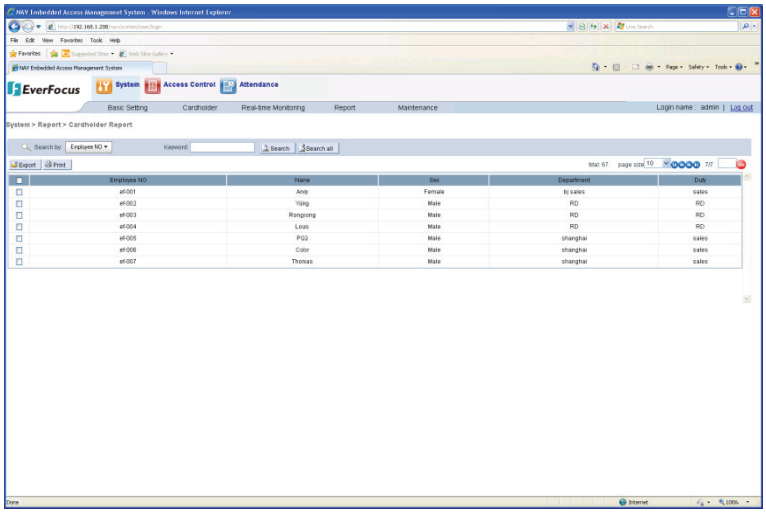


Figure10-7Search Cardholders

Input the employee number or name to do precise queries.

Search condition is divided into employee number, name. Input the keyword in the box, click the “Search” button, will show all the related results with keyword. Click “All” button, to get back to the all cardholder list. The query is exact and the results listed will fully match the keyword.

For example: There have two **cardholders** and their employee number are “ef-001” and “ef-002”,if just want to search “ef-001” as the result, input the key word “ef-001” into the search box and click search. The absence of any one character will be unable to query the cardholder.

10.3.2 Export Cardholders

Click the “Export” button, and the download file box will pop-up. All cardholders’ information will export to the CSV format, select the path to save the document. Click “OK” to confirm. Please see 7.1.7 Export function.

10.3.3 Print Cardholders

Click the “Print” button to enter to the cardholder printed page, for the specific operation methods see 7.1.8 Print function.

Chapter 11

11. Maintenance

11.1 Backup

Click the menu “System” → “Maintenance” → “Backup” to enter the backup page; shown below:

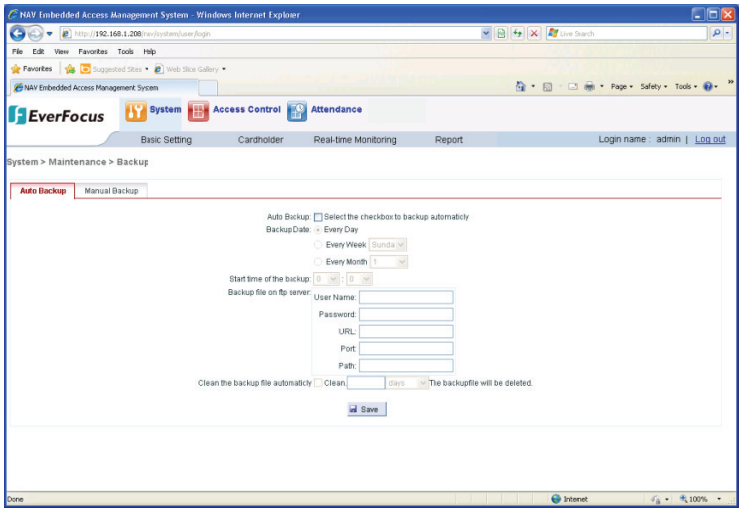


Figure11-1Backup

11.1.1 Manual Backup

Manual backup refers to backing up the system data. Select “manual backup” and click the “Backup” button. After a period of time, a system window will be shown to select a file path for saving the data to the local computer.

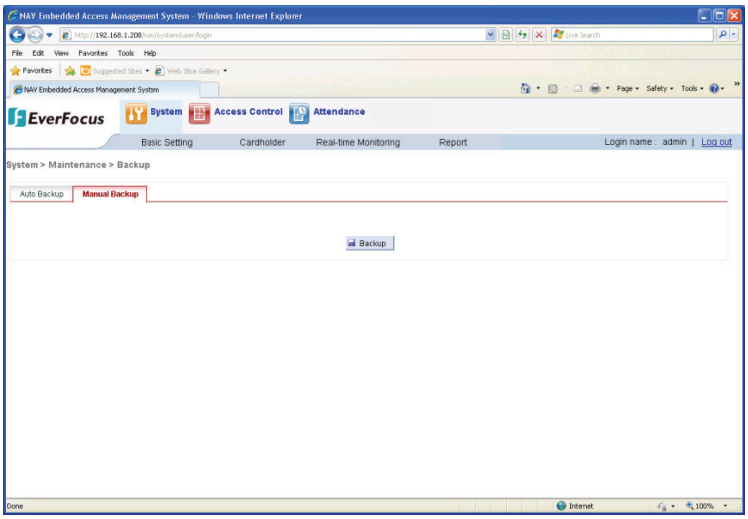


Figure11-2Manual Backup

11.1.2 Auto Backup

There are two ways to backup the data, manual and automatic. The automatic backup page is shown below:

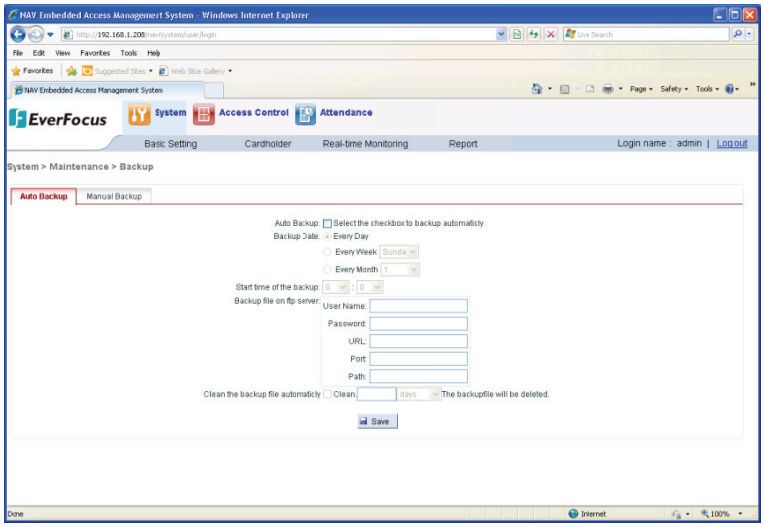


Figure11-3Auto Backup

Steps:

1) Click the “Auto Backup” tab and check the option to automatically backup.
2) Select the backup date and start time.
3) Enter the user name, password, URL, port, and file path of the FTP server to save the file.

   (FTP server is a remote server)
4) Select to delete the expired backup file.
5) Click the “Save” button to complete the auto backup settings.

11.2 Restore

Click “System”→ “Maintenance” → “Restore” to enter the page to restore data. The system provides two methods: Restore the database from a FTP server, or from the local computer.

11.2.1 Restore from a FTP Server

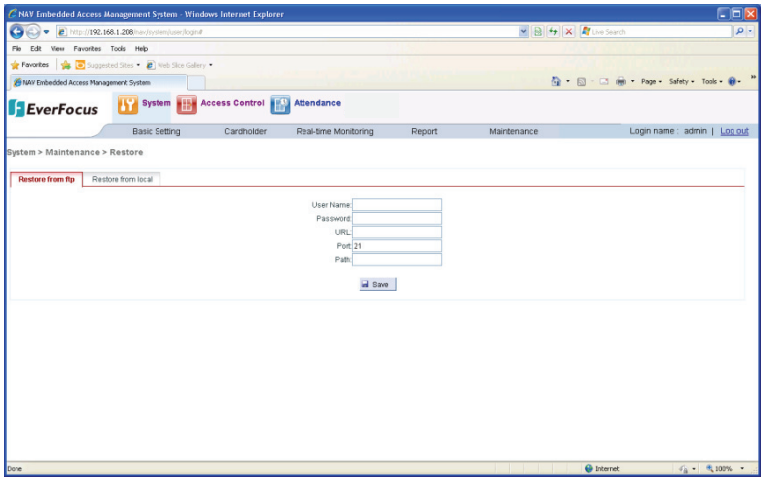


Figure11-4 Restore the Databasefrom a FTP Server

Steps:

1) Fill in the username and password to log in to the FTP server.
2) Input the FTP server’s URL, port, and file path (e.g.: abcd/nav_0808183801).
3) Click the “Save” button.

11.2.2 Restore from Local Computer

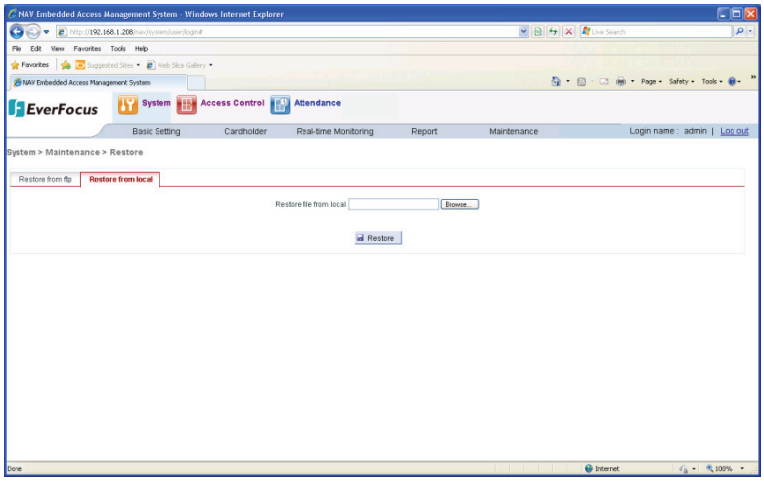


Figure11-5 Restore the Databasefrom Local

Steps:

1) Click the “Browse” button and select the database file to restore.
2) Click the “Restore” button to begin the restoration.

3) The system will display “restore the database succeeded.” when completed.

11.3 PurgeOut-of-date Data

Click on the menu bar “System” → “Maintenance” → “Purge Out-of-date Data”, to enter the purge page.

Chapter 12

12.Controller

This chapter describes how to set up controller. In this chapter you will learn:

- ✧ How to add and delete users, and configure the controller.
- ✧ How users download data from the controller.

12.1 Controller Setting

Click “Access Control” → “Controller” → “Controller setting” from the menu bar to enter the controller settings page, shown below:

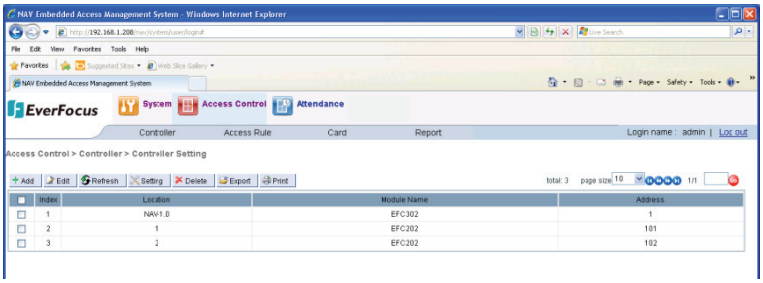


Figure12-1Controller Setting

On the controller setting page, the top is operation button list and the bottom is controller list.

- **OPERATION BUTTONS**

  Including the buttons to add, edit, refresh, setting (configure), delete, export and print.

- **CONTROLLER LIST**

  The controller list is showing all the controllers detail. Such as address, model number, location etc.

Note: It can only set the controller which is on line. Otherwise, it cannot configure the controller.

12.1.1 Add A Controller

Click the “Add” button, will pop-up a dialog box to add a controller, shown below:

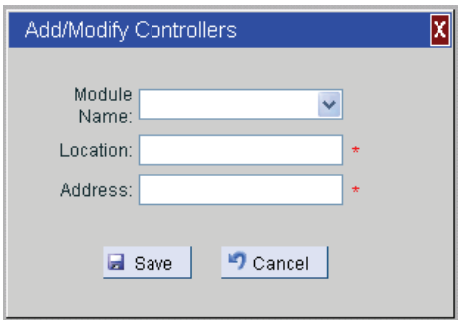


Figure12-2Add a Controller

Steps:

1) Select a model number in the selection box. Such as NAV-1.0 (EFC301, EFC302) etc.
2) Input location, address (4 digits).
3) Click the “Save” button, then it will search the controller on the network. If the controller is on line, the system will add it and display in the controller list. Otherwise, it will pop-up a dialog box, it shown as following:

Note: if the controller is on line, it cannot be added by the system software. Please make sure the controller is online before add it.

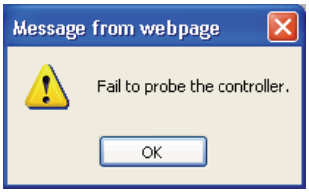


Figure 12-3 Fail to Add aController

12.1.2 Edit A Controller

Select the controller to be edited in the controller list. Click the “Edit” button, it will pop-up the Add/Modify dialog box. It shown below:

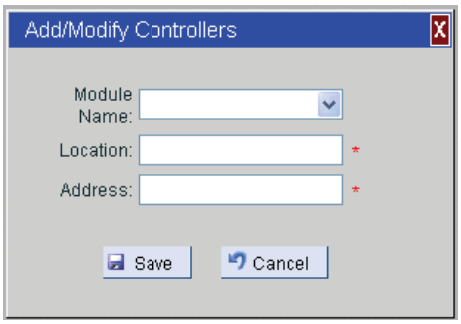


Figure12-4Edit a Controller

Steps:

1) Edit model number, location and address.
2) Click the “Save” button to save the settings.
3) Click the “Cancel” to cancel.

12.1.3 Delete A Controller

Select the controller to be deleted from the list, click the section box, the row's background will be green, then click the "delete" button to delete.

12.1.4 Refresh

Choose a controller in the list, click the "Refresh" button, it will get its configuration from the controller.

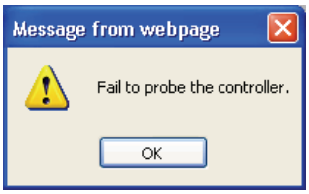


Figure12-5Refresh a Controller

Click the "ok" button to confirm.

12.1.5 Setting

Select a controller to be configured, then click the "Setting" button, enter the settings page, shown below:

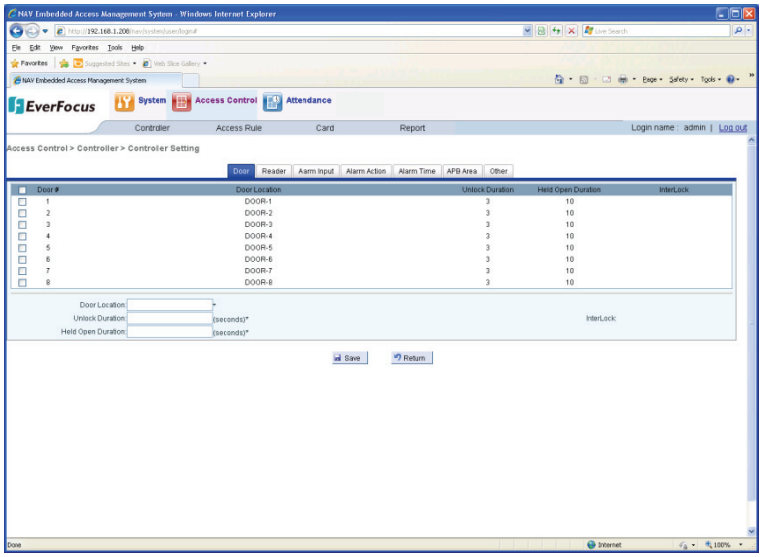


Figure12-6Controller Setting

In the controller setting page, users can configure all the features such as door, reader, alarm input, alarm action, alarm time, APB area and other settings. The following will explain the settings.

12.1.5.1 Door

Including door location, door unlocks time and door held open time.

Door Location: Description of the door location.
Door Unlock Time: Set the door open time when a valid card is swiped or the Request-to-Exit button is pressed. The door remains open as long as the RTX button is pressed down. The door open time does not count until the button is released. If two cards are swiped successively, the door open time does not count until the second card has been swiped. The default time is 3 seconds. The maximal door open time is 59999 seconds.
Door Held Open Time: Door sensor monitors the open/close status of a door. If "unlock" is not set by the system (door is normally considered closed), then door should close after opening. It is considered abnormal if controller does not receive the door close signal from door sensor for a reasonable amount of time after the door is opened. This time period is call door held open time or door over time. According to this setting, the controller will determine whether to generate an alarm or not after the door sensor timeouts. The default value of door held open time is 5seconds. The maximal door held open time is 59999 seconds.

Steps:
1) Select the door page.
2) Click the door which needs to be set.
3) Input door information including: door location, unlock duration, held open duration, interlock etc. If two or more doors are interlocked, they cannot be opened the same time. If one of the interlocked doors is open, the other doors cannot be opened until the first door is closed. In short, there can be only one door open at any time point among interlocked doors. User can set interlock function when an interlock compatible controller controls two or more doors. This setting is particularly suitable to environment that requires high-level security, such as banks and prisons.
4) Click the "Save" button to save your changes.

12.1.5.2 Reader

Settings page for the reader number, name, door location, keypad reader, system reader, input time for keypad, in/out type, source and destination area etc.

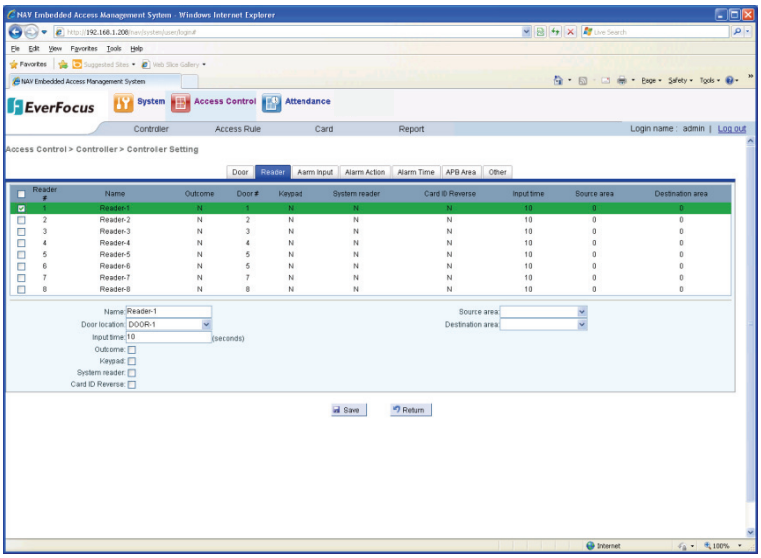


Figure12-7Reader

Reader No.: the number of the selected reader
Door location: description of the actual location of the door to which the reader is installed. The default setting is that each reader is installed to the door with the same number.
Reader name: name of the reader.
Keypad reader: whether the current reader is a keypad reader. For a keypad reader, if a card PIN is enabled and the verification level is “card plus PIN”, one must enter card PIN using the keypad to gain access to the door.
System reader: whether the current reader is a system reader. A system reader can transmit a card number to the controller to enroll cards to the controller. Any reader connected to the controller can be set as a system reader.
Input time: when the verification needs to input a password, the max waiting time for inputting the password input. If more than the time, the controller display will go back to main screen.
In/Out type: whether the reader is an entry reader or an exit reader.
S**ource area and Destination area:** These settings are for APB function. Refer to Anti-Passback (APB) page for details.

Steps:

1) Click the reader tab page.
2) Select the reader which needs to be set.
3) Input reader information including: reader name, door location, input time, keypad reader, system reader, source area, destination area etc.
4) Click the “Save” button to save your changes.

12.1.5.3 Alarm Input

Including name, whether fire alarm input, input mode, output mode, delay time, alarm output time, door behavior under fire alarm.

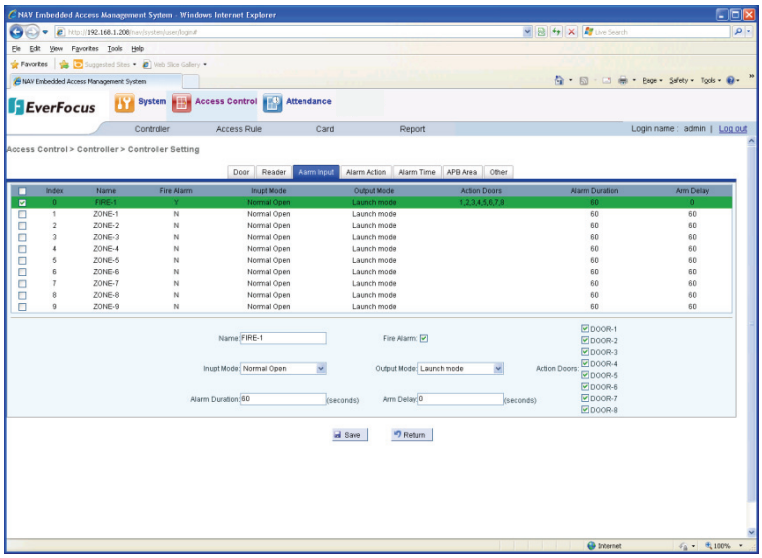


Figure12-8Alarm Input

Alarm Input Name: rename the alarm input
Fire Alarm: "Yes" means the alarm is a fire alarm, "No" means it is not a fire alarm. The first alarm input is default as a fire alarm and cannot be modified.
Alarm Input Mode: "Invalid" means the current alarm input is disabled. "Normally Open" means the circuit disconnects in the normal condition (i.e. without input) and an alarm will be triggered if circuit connects with inputs. "Normally close" is the opposite.
Alarm Output Mode: "Lock" mode means an alarm output is triggered if there is an alarm input. Once triggered, the alarm output remains till the alarm output time has elapsed or being reset manually. If the alarm input signal lasts longer than the alarm output time, anew alarm output will be triggered. "Direct" mode means there will be an alarm output as long as there is an active input signal; the alarm outputs stops when the input signal stops.
Alarm Delay Time (s): in the range of 1-59999 seconds
Alarm Output Time (s): in the range of 1-59999 seconds
Alarm Output: the terminal(s) of the alarm output
Door Module Output: the terminal(s) of the door module for the alarm output
Door behavior under fire alarm: when doors are open during fire alarm.

Steps:

1) Click the "alarm Input" tab page.
2) Select the input which needs to be set.
3) Input alarm input information including: alarm input name, whether fire alarm input, input mode, output mode, alarm delay time, alarm output time, door module output, door behavior under fire alarm etc.
4) Click the "Save" button to save your changes.

12.1.5.4 Alarm Action

On the alarm action settings page, users can configure the alarm output, including: the main modules output, door module output and alarm module output etc.

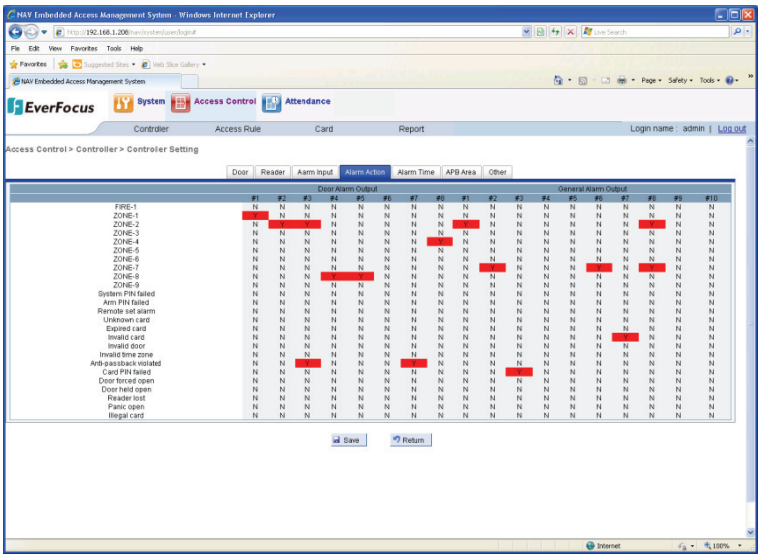


Figure12-9Alarm Action

A NAV controller consists of two basic components: the main module and the door module. User can install up to 4 door modules and 1 alarm module. These three types of module are all equipped with alarm function.

Main module has 2 alarm inputs (figure 12.9 fire-1 and Zone-1), they response for fire alarm and tamper alarm. It also has2 alarm outputs, corresponding to main alarm output and auxiliary alarm output.

Each door module has 2 alarm outputs, which usually react to alarm events on the corresponding door. However, it can be set to react to other alarm events as well. Alarm outputs on the door module can connect up to 5A external alarm devices.

Alarm module has 8 inputs and 8 alarm outputs, 8 alarm inputs can be connected to an external alarm input devices, such as PIR motion sensor, glass break sensors, etc. 8 alarm output can be connected to the maximum current 2A (amps) and external alarm device.

NAV controllers keep tracking all events in the access control system, whether allowed or disallowed, normal or abnormal. For example, all granted access events and all denied access events are recorded.

Some events are critical which must trigger the alarm output, like the firm alarm input, the zone alarm input, etc. But some events are not important and should not trigger an alarm output, like denied access due to an invalid time. These settings all depend on the users' requirements. The controller collects all events that might trigger the alarm output and provides the full capacity to enable or disable the alarm output based on these events.

Sometimes a user may wish to allocate a particular event to a particular alarm output, or allocate alarm inputs in certain area to multiple alarm outputs. The Flex controller delivers all the function and flexibility needed to do so. Users can define whether certain event will trigger an alarm, and can further specify to which alarm output that event is allocated.

An alarm can be triggered by events such as fire alarm, zone alarm 1~8, unknown card, expired card, invalid card, invalid door, invalid time, card APB fail, card PIN fail, SYS PIN fail, ARM PIN fail, door forced open, door held open, reader lost, alarm input 0, and remote alarm.

All these events can be allocated to any alarm relay output on main module, door module and alarm module. Alarm output setting interface is given in a table format and every column represents an alarm output source. The alarm output is shown in a drop-down menu.

If there are two options in the drop-down menu, it means the alarm output is not related to door. “Yes” indicates there is alarm output (relay energized), “No” indicates there is no alarm output (relay not energized).

If there are three options in the drop-down menu, it means the alarm output is related to door. “Y” indicates there is an alarm output (relay energized), “N” indicates there is no alarm output (relay not energized), “R” refers specifically to alarm output relay on the door module, indicating that alarm output will be generated only if the events occurs on the corresponding door module.

- **Zone Alarm:** The zone alarm reacts to 8 alarm inputs on the alarm module. Any events in the arm zone may trigger a zone alarm event. The controller generates an alarm output according on the setting in the “Zone Alarm” column.

- **Fire Alarm:** A fire alarm event is generated when there is a fire alarm input. The controller generates an alarm output according on the setting in the “Fire Alarm” column.

- **System PIN Fail:** User is required to enter system PIN to enter to the system setting menu. If an incorrect system PIN is entered three times consecutively, the system will generate a “system PIN fail” event. The controller generates alarm output(s) according to the setting in the “system PIN fail” column.

- **ARM PIN Fail:** User is required to enter ARM PIN when pressing the “ARM” key on the controller to arm/disarm the system. If an incorrect ARM PIN is entered three times consecutively, the system will generate an “ARM PIN fail” event. The controller generates alarm output(s) according to the setting in the “ARM PIN fail” column.

- **Tamper Alarm:** A tamper alarm event will be generated if there is a temper alarm input. The controller generates alarm output(s) according to the setting in the “Tamper Alarm” column.

- **Remote Alarm:** A system administrator can directly generate alarm signals using the control software when he observes an abnormal condition through a surveillance system. This is defined as a Remote Alarm event. The controller generates alarm output(s) according to the setting in the “Remote Alarm” column.

- **Unknown Card:** unknown card refers to a card that is never enrolled in the system. An unknown card event will be generated when an unknown card is presented to any reader. The controller generates alarm output(s) according to the setting in the “Unknown Card” column.

- **Expired Card:** any card in the system is usually assigned a valid date. After the valid date passes, the controller will automatically set the card as an expired card. An expired card cannot gain access to the system. An expired card event will be generated if an expired card is swiped on the reader. The controller generates alarm output(s) according to the setting in the “Expired Card” column.

- **Invalid Card:** User can directly set a card as an invalid card to disable the card. An invalid card cannot gain access to the system. An invalid card event will be generated if an invalid card is swiped on the reader. The controller generates alarm output(s) according to the setting in the “Invalid Card” column.

- **Invalid Door:** Each card belongs to an access group. For each group, the system can assign access rights to certain doors for certain time zones. An Invalid Door event will be generated

when a card is swiped at any door at which it does not have the right to pass. The controller generates alarm output(s) according to the setting in the “Invalid Door” column.

- **Invalid Time:** Each card belongs to an access group. For each group, the system can assign access rights to certain doors for certain time zones. An invalid time event will be generated if a card is swiped during a time period in which it does not have the right to pass. The controller generates alarm output(s) according to the setting in the “Invalid Time” column.

- **APB Fail:** If the card APB property is enabled, and door behavior under APB is set to “unlock”. A cardholder will be able to enter/exit any doors by swiping the card. The system generates an APB fail event if an APB event is triggered. The controller generates alarm output(s) according to the setting in the “APB Fail” column.

- **Card PIN Fail:** A card PIN fail event is generated when a PIN-enabled card is presented at a reader and an incorrect PIN is entered three times consecutively. The controller generates alarm output(s) according to the setting in the “Card PIN Fail” column.

- **Door Forced Open:** A door forced open event is generated when the door sensor indicates to the controller that a door is opened, but no legitimate card has been presented and a Request-to-Exit button has not been pressed. The controller generates alarm output(s) according to the setting in the “Door Forced Open”. In practice, a door forced open event will be generated if a door is kicked open.

- **Door endures Open:** A door endures open event is generated if a cardholder enters endures PIN to unlock a door when under endures. The controller generates alarm output(s) according to the setting in the “Door endures Open”.

- **Door Held Open/Overtime:** the system keeps tracking of the door status when a card is presented to a reader or Request-to-Exit button is pressed. A door held open/overtime event occurs when a door is held open for longer than the allowed door held open time. The controller generates alarm output(s) according to the setting in the “Door Held Open” column.

- **Reader Lost:** A reader lost event is generated when the controller detects that the card reader appears to have been disconnected from the system. The controller generates alarm output(s) according to the setting in the “Reader Lost” column.

- **Panic door:** When an access denied appears and request open did not implement, however, door magnetic sensor is displayed the door have been opened, it will lead a “panic door” event. The controller generates alarm output(s) according to the setting in the “Panic Door” column.

Steps:

1) Click the “Alarm Action” tab page
2) Select an alarm to be set in alarm list.
3) In the corresponding, click the position to show drop-down menu of alarm output, select the output value: R, Y, N.
4) Click the “Save” button to save your changes.

12.1.5.5 Alarm Time

On the alarm time setting page, users can set the alarm time for the specified controller.

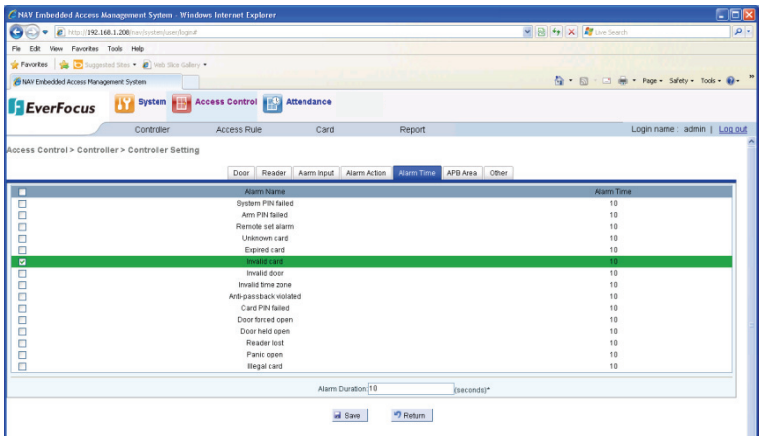


Figure12-10Alarm Time

Steps:

1) Click the “Alarm Time” tab page
2) Select an alarm to be set in alarm list.
3) Input alarm time.
4) Click the “Save” button to save the change.

12.1.5.6 APB Area

On the APB Area page, users can configure the APB area, including: area name, Enable or not, open door when APB check fail or not.

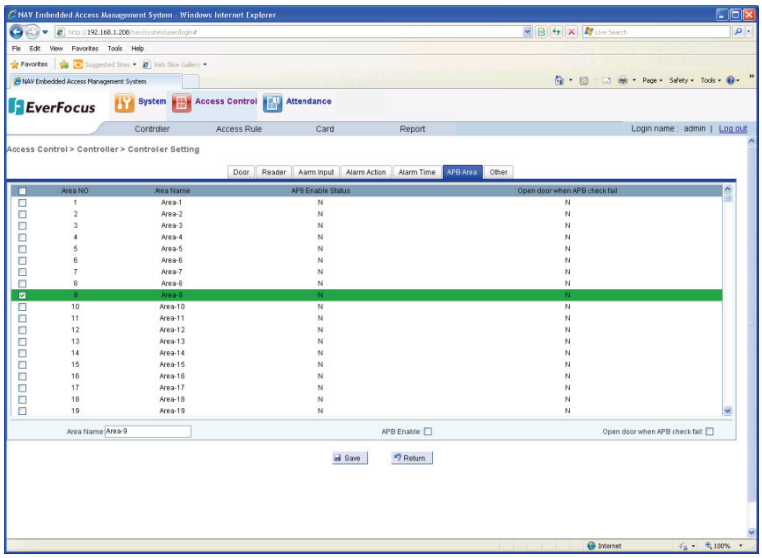


Figure12-11 APB Area

APB area setting is to edit arm zone name for the selected controller. When placing mouse on top of an arm zone in an electrical map, the name of the arm zone will be shown.

Steps:

1) Click the “APB area” tab page.
2) Select an area to be set.

3) Input area information.
4) Click the “Save” button and save the changes.

12.1.5.7 Other Setting

In other setting page, it is for the overall setting of the controller. The setting is including first-card-In, time synchronization server, date format, daylight saving time etc.

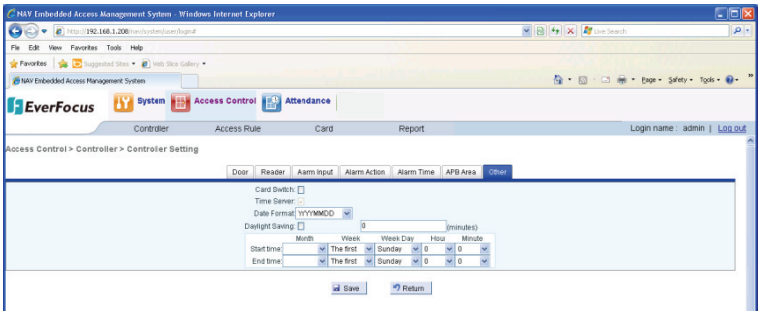


Figure12-12Other Setting

- **First-card-IN:** choose from enabled or disabled. When first-card-in is enabled, in a door zone of which the schedule is set as “normally open”, only after a first-card enabled card has been presented to the reader, will other cards be able to unlock the door.
- **Time synchronization server:** indicates whether the controller is the time synchronization server in the system. All controllers in the system will automatically adjust its date and time setting to match that of the time synchronization server. There can be only one time synchronization server in the system and the last assigned time synchronization server will replace any previous setting. If the controller is connected to a PC installed with Flex software, the software will automatically modify the controller date and time to match the PC setting. If the controller date and time are found to be incorrect, check the date and time on the control PC.
- **Date format:** the system offers two date format: “YYYY-MM-DD” and “MM-DD-YYYY” and users can choose the desired format.
- **Daylight saving time:** Whether auto Daylight Saving Time (DST) is enabled. When auto DST is enabled, user need define the start and end dates of DST, including month, week, date, and time, forward or backward. When auto DST is enabled, the controller will automatically adjust DST one hour forward from 1:59:59am to3:00:00am on the first Sunday in April, and adjust it backward one hour from1:59:59am to 1:00:00am on the last Sunday in October.

Steps:

1) Click the “Other” tab page.
2) Select and change the setting.
3) Click the “Save” button to save the changes.

12.1.6 Export Controllers

Click the “Export” button, pop-up download file box, all controllers will be exported to CSV format, select a path to save the file. Click “OK” to confirm. Please see 7.1.7 Export function.

12.1.7 Print Controllers

Click the “Print” button to enter to the printing page, the specific operation method see 7.1.8 Print function.

12.1.8 Download Data to Controller

Click on the menu bar “Access Control” → “Controller” → “Download Data to Controller”, shown as following:

Figure12-13 Download Data to Controller

The page is divided into left and right columns. Left is data options list and right is controller list.

- **Data option list:** Includes card data, access rule, day setting and controller configuration.
- **Controller list:** Display all the current controllers.

Download Data: Download data of card, access schedule, day setting and controller configuration to the specified controller.

Steps:

1) Select the data from the list to be downloaded to the controller.
2) Select the controllers from the controller list.
3) Click the “Download” button, completely operated.
4) The “Download” button, completely operate.

Chapter 13

13. Access Rule

13.1 Date Type

Click “Access Control” → “Access Rule” → “Date Type”, enter to the date type page, shown as following:

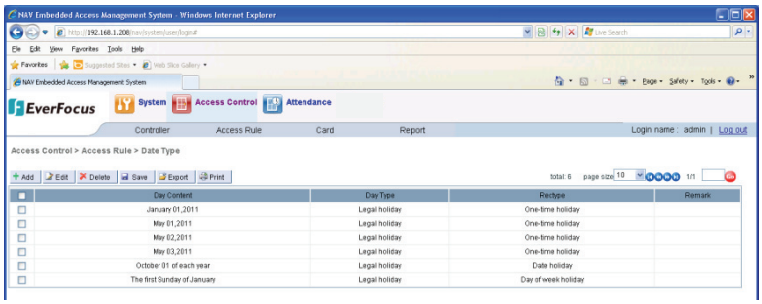


Figure13-1Date Type

13.1.1 AddA Date

In the date type page, click the “Add” button and will pop-up below screen:

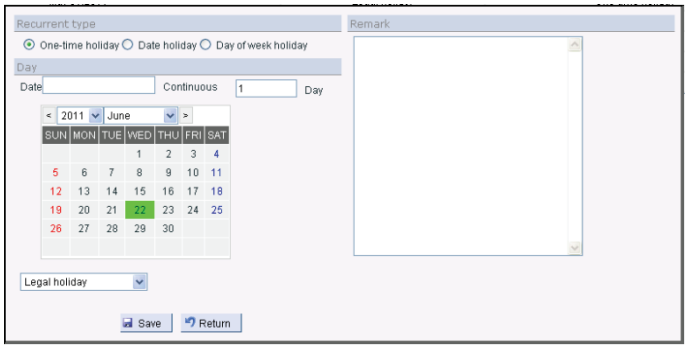


Figure13-2Add a Date

Controller supports 10 date types, including: Sunday to Saturday (7 types), custom 1-3. Sunday to Saturday is automatically set based on the calendar. Users can customize according to their own needs custom 1-3. In this manual, custom 1-3 are holidays. Holiday setting is these 3 holiday type. The NAV controller supports up to 255 holiday setting.

- **Recurrent type**

Software allows set the holiday flexibility in accordance with the standard set of three different Holiday. There three types of cycles are as following:

✧ **One-time holiday:**

A one-time holiday is a holiday that will occur once, and will not recur in subsequent years. An example is a company organized travel event during Oct. 10, 2008 to Oct. 15.

✧ **Date Holiday**

A date holiday is a recurrent holiday that occurs on the same date every year. For instance, the New Year holiday, which occurs on January 1, is a date holiday

✧ **Day of week Holiday**

Day of week holiday is another recurrent holiday type. It defines a certain day of a certain week, in a certain week of a month. Thanksgiving is an example of a Day of Week holiday, falling on the 4th Thursday of November

! Note: These holidays setting should be complete when controller first time to be used, and re-checked at the beginning of each year.

Steps:

1) Select day of recurrent type.
2) Select the date in calendar.
3) In the day of type, select the type day.
4) Input the day of notes content (optional)
5) Click “Save”, new date will save it to the system.

13.1.2 Delete A Date

Steps:

1) Select the holiday which need to delete in the setting page.
2) Click the “Delete” button and confirm if sure to delete.
3) Click “Ok” to delete.

Note: after added and delete operations, the system will automatic save the revised information.

13.2 Group Schedule

Click on the menu bar, select “Access Control” → “Access Rule” → “Group Schedule”, for the Group Schedule page, shown as follows:

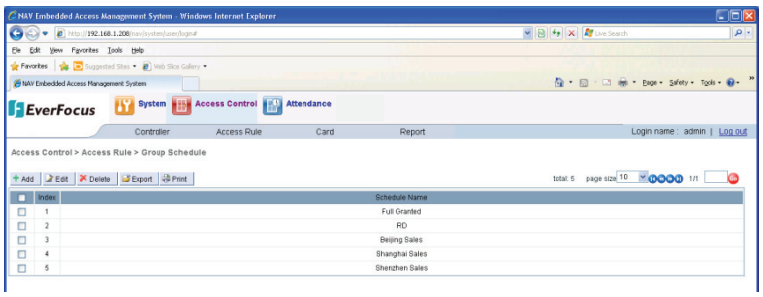


Figure13-3User Group Schedule

13.2.1 Add A Group Schedule

In the group schedule setting page, click the “Add” button to add a new schedule.

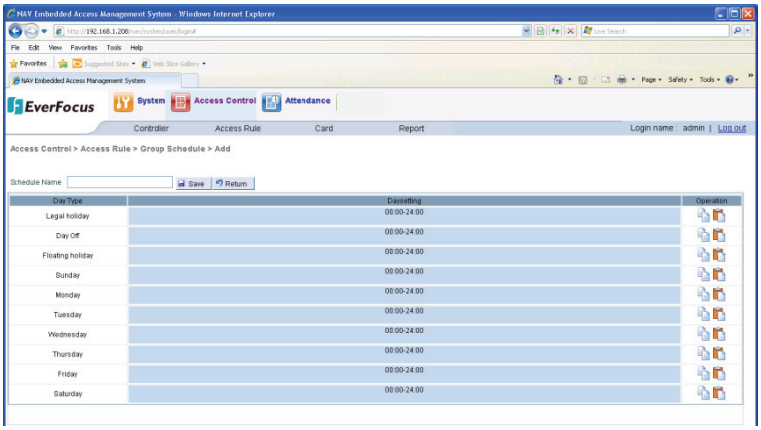


Figure13-4Add a Group Schedule

Steps:

1) Enter a new name on the box.
2) Click on one cell in the column “Day setting”, pop-up a box where can set the time sections and entry/exit mode, shown as Figure13-5.
3) After completed, click the “save” button and the new group schedule have been created.

13.2.2 Delete A Group Schedule

Steps:

1) In the group schedule setting page, select one or more schedule to be deleted.
2) Click the “Delete” button.
3) Confirm to delete.
4) Click the “Ok” button.

13.2.3 Edit A Group Schedule

Select a group schedule and click the “Edit” button, enter to the group schedule setting page, shown as following:

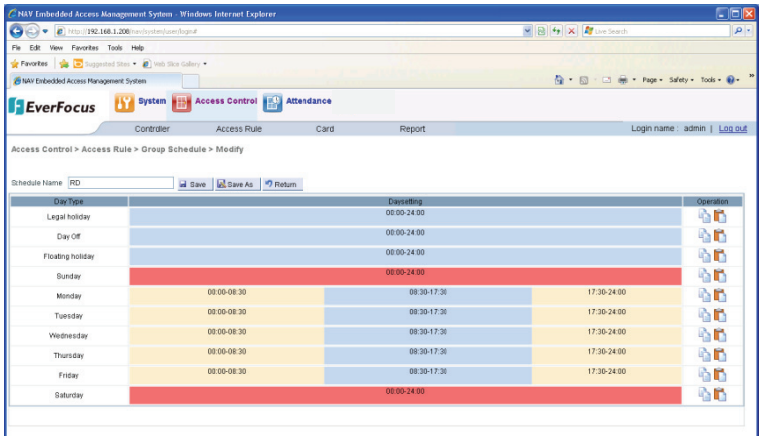


Figure13-6Edit a Group Schedule

The default entry/exit mode is “Card only”, if need to set the mode in different time sections, click the time bar, enter to the “Modify Schedule” page, shown as following:

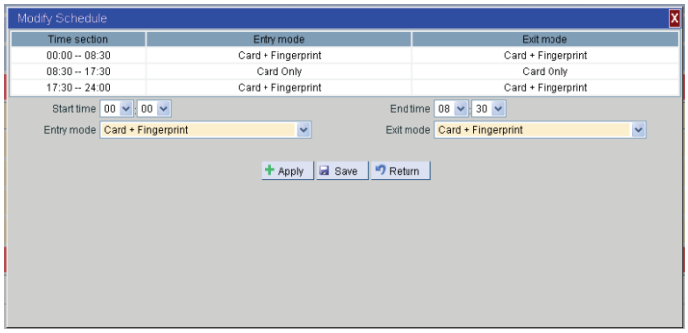


Figure13-7Modify a Schedule

Input the start and end time, select the entry/exit mode for current time section, and click the “Apply” and “Save” button. Click “Return” back to group schedule setting page.

After back to the page, click “Save” button, group schedule have been saved, shown as following:

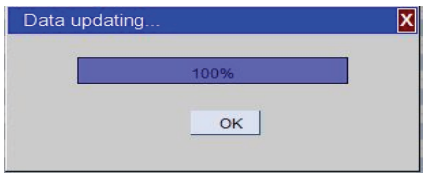


Figure13-8Data Updating

After the current date type is set, the user want to be set the other date as same, just need to click the “copy” button to copy the pervious setting in the “Operation” column of the first one, and then click the “paste” button for the second one, the setting will be applied to the second one.

13.2.4 Save As A New Schedule

A group schedule can be edited and it can be saved as a new schedule. This feature is used to add a similar setting for other group schedules.

Steps:

1) Edit the schedule name on the box or not.
2) Click “Save as” to create a new schedule.

13.3 Access Group

Click the menu “Access Control” → “Access Rule” → “Access Group”, to enter the access group setting page, shown as following:

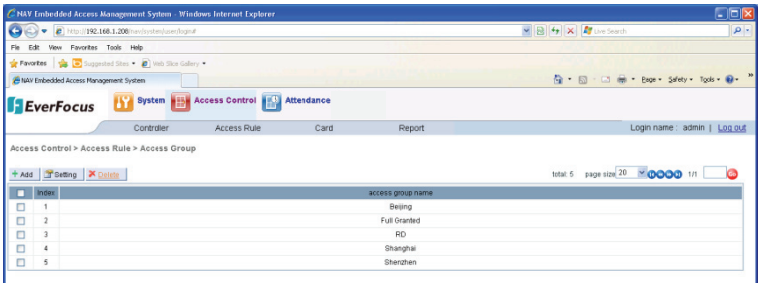


Figure13-9Access Group

13.3.1 Add A Access Group

In “Access Group” page, click the “Add” button, the group setting screen pop-up.

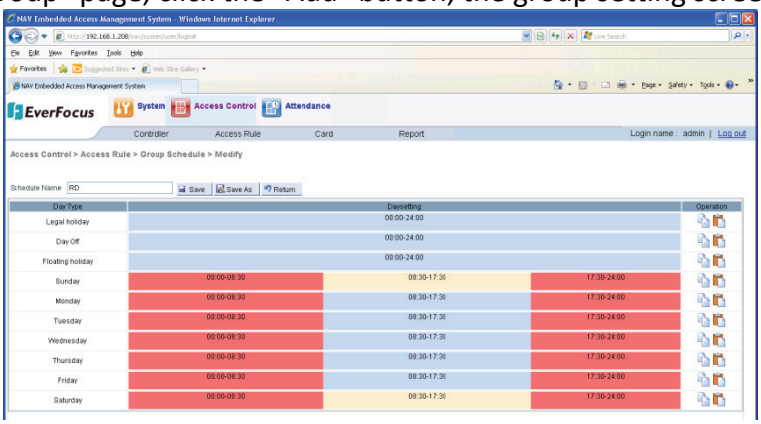


Figure13-10Add a Access Group

Steps:

1) Enter a new group name.
2) Select each door’s unlock level, group schedule (or following door’s schedule).
3) Click “Save” and return to the setting page.

13.3.2 Delete A Access Group

Steps:

1) Select one or more access group to be deleted.
2) Click the “Delete” button.
3) Confirm to delete.
4) Click “OK”.

13.4 Door Schedule

Click on the menu bar “Access Control” → “Access Rule” → “Door Schedule”, to enter the door schedule setting page, shown as following:

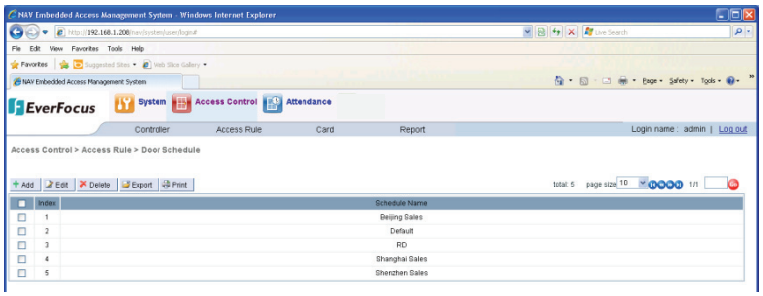


Figure13-11Door Schedule

13.4.1 Add A Door Schedule

On the door schedule setting page, click the “Add” button to enter to the setting page.

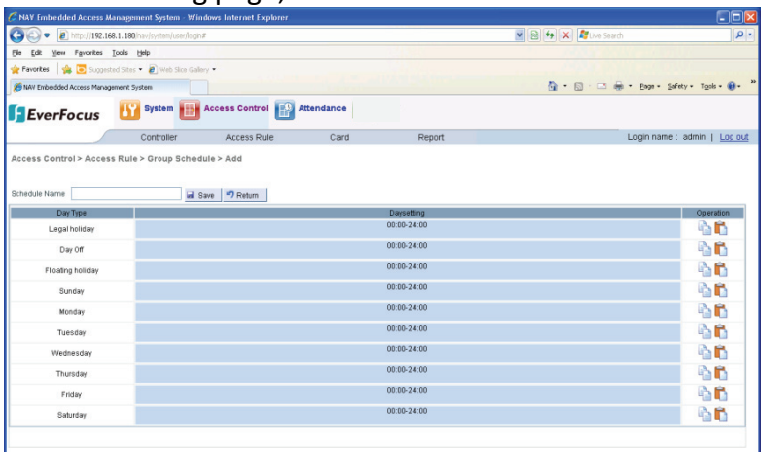


Figure13-12Add a Door Schedule

Steps:

1) Input a new schedule name in the text box.
2) Click on one cell in the column “Day setting”, pop-up a box where can set the time sections and entry/exit mode, multi-card for each door, shown as Figure13-13.
3) After completed, click the “save” button and the new door schedule have been created.

13.4.2 Delete A Door Schedule

Steps:

1) In the door schedule setting page, select one or more schedule to be deleted.
2) Click the “Delete” button.
3) Confirm to delete.
4) Click the “Ok” button.

13.4.3 Edit A Door Schedule

Select a door schedule and click the “Edit” button, enter to the door schedule setting page, shown as following:

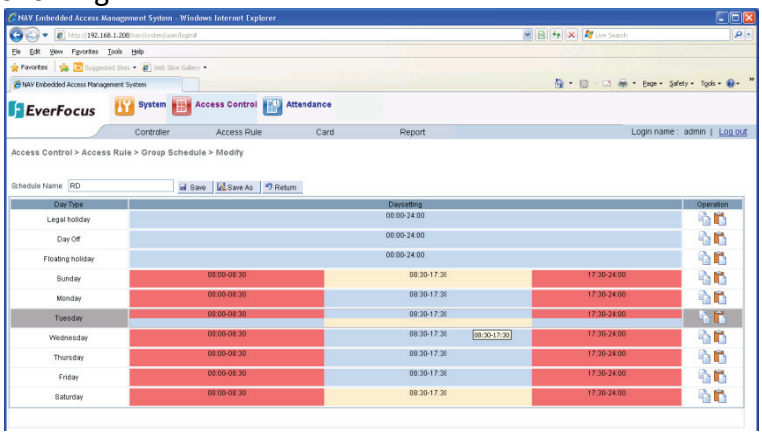


Figure13-13 Edit a Door Schedule

The default entry/exit mode is “Card only”, if need to set the mode in different time sections, click the time bar, enter to the “Modify Schedule” page, shown as following:

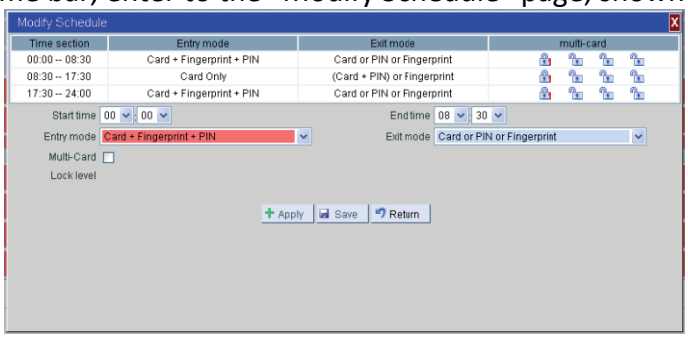


Figure13-14Modify Schedule

Input the start and end time, select the entry/exit mode for current time section, set the lock level for the door if using the multi-card access, and click the “Apply” and “Save” button. Click “Return” back to group schedule setting page.

After back to the page, click “Save” button, door schedule have been saved, shown as following:

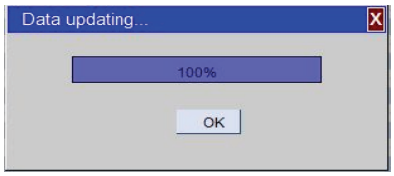


Figure13-15Data Updating

After the current date type is set, the user want to be set the other date as same, just need to click the “copy” button to copy the pervious setting in the “Operation” column of the first one, and then click the “paste” button for the second one, the setting will be applied to the second one.

13.4.4 Save As A New Schedule

A door schedule can be edited and it can be saved as a new schedule. This feature is used to add a similar setting for other door schedules.

Steps:

1) Edit the schedule name on the box or not.
2) Click “Save as” to create a new schedule.

13.5 Access Door

Click on the menu bar “Access Control” → “Access Rule” → “Access Door”, for the access door settings page, shown as following:

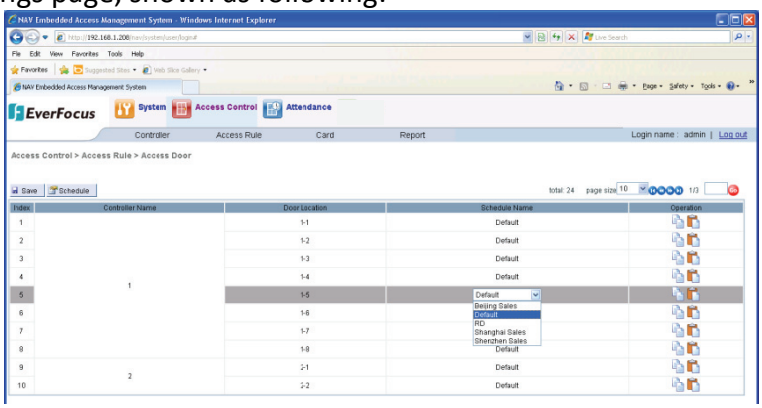


Figure 13-16Access Door

Steps:

1) Select a door schedule for each door
2) After completed, click the “Save” button. It will display a “Modify successfully” message when completed.
3) Click the “Ok” to confirm the data update.

The user can also use the function “copy” and “paste” between different doors, the two doors will be used the same door schedule.

Chapter 14

14. Card

This section describes how to add, edit cards, through this section you will learn:

- Card Type Setting
- How to add, delete and edit one or more cards.
- Import cards to the controller

14.1 Card Type Setting

Click on the menu bar “Access Control” → “Card” → “Card Type Setting”, enter to the card typesetting page, shown as following:

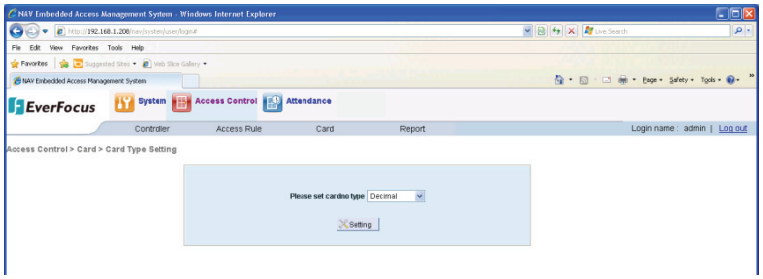


Figure14-1Card Type Setting

Card type means the serial number’s format of the cards added or to be added to the controller will be shown to the user type through the software. There are three types: decimal, hexadecimal, nnn-nnnnn.

- ✧ **Decimal:** indicates an 8-digit decimal card number with each d represents a decimal number of 0-9. The form is a continuous 8-digit decimal number. An example of this type is "00492423".
- ✧ **Hexadecimal:** indicates a 6-digit hexadecimal card number with each one represents a hexadecimal number of 0-9, A-F. The form is a continuous 6-digithexadecimal number. Examples of this type are "44EA5B" and “256871”.
- ✧ **nnn-nnnnn:** indicates an 8-digit decimal card number with each d represents a decimal number of 0-9. The form is divided into two parts with the first part of a3-digit decimal number (high), and the latter part of a 5-digit decimal number (low).The two parts are spaced by symbol "-" or a space. Examples of this type are "07509039 " and “154-58742”.

Select the card type in the drop down menu, and click the “Setting” button.

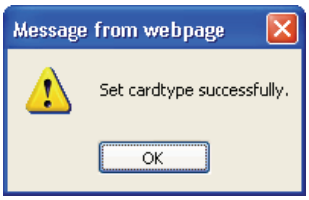


Figure14-2Setting Successfully

14.2 Card Setting

Click on the menu bar “Access Control” → “Card” → “Card Setting”, enter to the card setting page, shown as following:

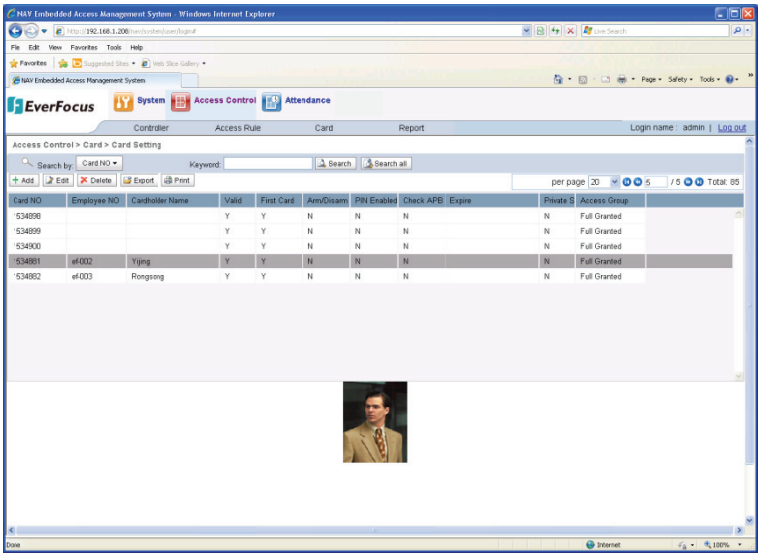


Figure14-3Card Setting

In the card setting page, the top is query area and operation button list, the below is card list.

- **Query Operation Area:**

Select a search field and input the search criteria in the “keyword” text box, click the “Search” button to start searching. If there are cards matching, they will be shown in the card list.

- **Operation Button List:**

Including add, edit, delete, export and print buttons, used to operate the card.

- **Card List:**

Shown all the card information including: card number, employee number, cardholder name, access group and its properties etc.

14.2.1 AddA (Batch) Card

In the card setting page, click the “Add” button and pop-up a window, shown as following:

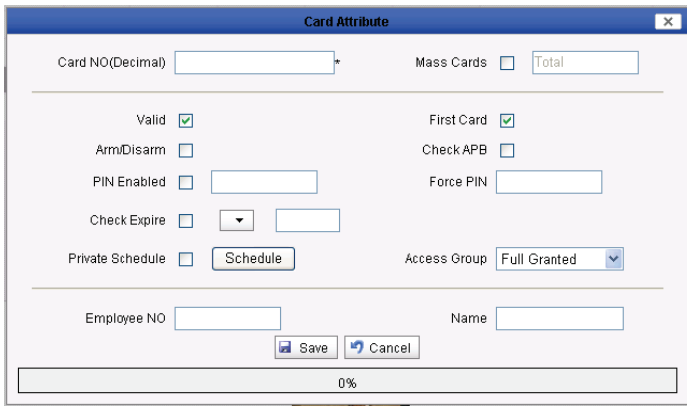


Figure14-4Add a (batch) Card

Steps:

1) In the window, input the card number, if users want to add more than one card that its serial number is consecutive, please check the “Mass Cards” first, and then input the batch number, the inputted serial number will be as the start number.
2) Set the card’s properties including valid, first card, arm/disarm, APB, password status and use the expiration etc. then input the password and force PIN , select the access group, if using the card’s schedule, please check the “Private Schedule” first.
3) Assign one or more cards to one cardholder, after inputted the employee number, the matched name will automatically pop-up, click to select it. Empathy the user can also input employee name first.
4) Click the “Save” button, the card will be added to the list.

Note: The details about added, modified and deleted operations please refer to 5.2.19.

Card number: Input the number, the software supports three kinds of card type. Each type will be converted to according format. Use 10 decimal to be a sample, if its length is shorter than 10, the software will add “0” at the beginning of the number.

ID card is Wiegand-26 format, which means 26 bits. Discarded the first 2 and last 2 parity numbers, the remaining 24 digit will be converted to 10 decimal.

- Users can read the number printing on the card.
- Swipes the card on the reader, then user can find the card number in the access denied record list on monitoring event page of the software.
- The card can be added to the controller by the system reader in the controller’s menu.

If the added cards’ quantity is more one which number is continual, input the starting number and quantities to batch add.

14.2.2 EditA (Batch) Card

Edit a Card: In the card setting page, click the card which needs to be edited, pop-up a window, shown as following:

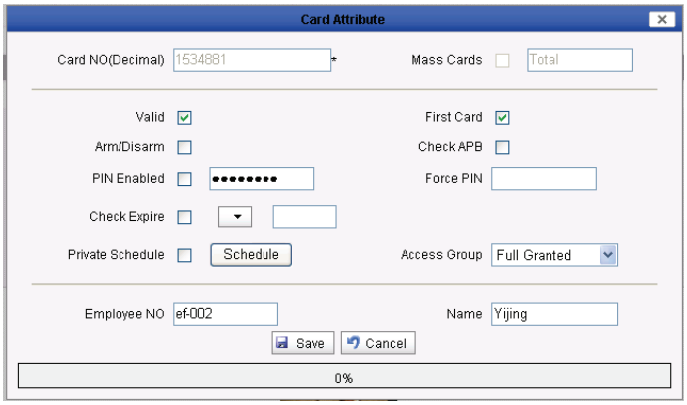


Figure14-5Edit a Card

Modify the relevant properties of the card, select and click the “Save” button, when the progress bar becomes 100%, click the “Back” button to close the window.

Edit batch Card: Press the Shift key to select more than one cards, click the “Edit” button and pop-up a window to modify the relevant attributes. Click the “Save” button after edit. Click the “Back” button to close the window.

14.2.3 Delete A (Batch) Card

Steps:

1) In the card setting page, select the cards which need to be deleted.
2) Click the “Delete” button.
3) Confirm to delete.
4) Click “OK” to finish.

14.2.4 Export Cards

Click the “Export” button, pop-up download file box, all cards will be exported to CSV format, select a path to save the file. Click “OK” to confirm. Please see 7.1.7 Export function.

14.2.5 Print Cards

Click the “Print” button to enter to the printing page, the specific operation method see 7.1.8 Print function

14.2.6 Search Cards

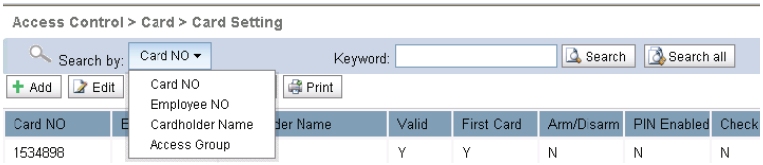


Figure 14-6 Search Cards

Select a search field and input the search criteria in the “keyword” text box, click the “Search” button to start searching. If there are cards matching, they will be shown in the card list. Click “Search All” button, back to the all card list.

14.3 Import Cards

Select System menu bar “Access Control”→ “Cardholder” → “Import Cards”, and then enter to import page, shown as following:

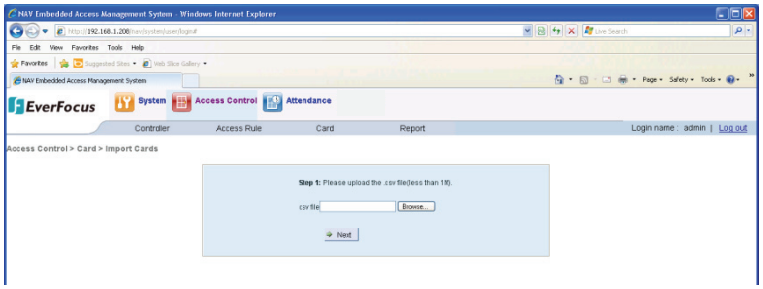


Figure14-76 Update Excel File

Steps:

1) Upload Excel format file, click the “Browse” button, and locate the file want to upload. Imported file must be CSV format (Excel 97-2003), and less than 1M.
2) Click the “Next” button to enter to the operation page, shown as following:

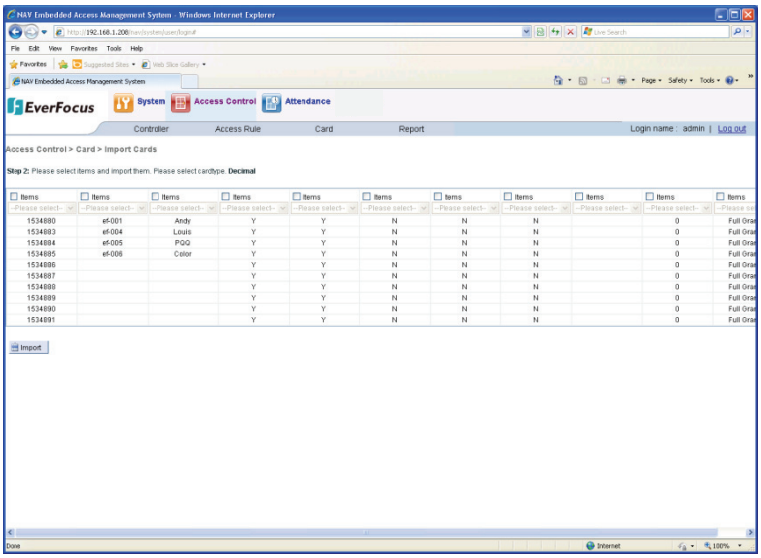


Figure14-8 Import Cards

1) Click the drop-down menu of attributes, and select the corresponding attribute categories, and check the attribute box on the top of column.
2) Click on “Import”, system starts to import the cardholders.
3) Displayed after the completion of “xxx records have been imported.”

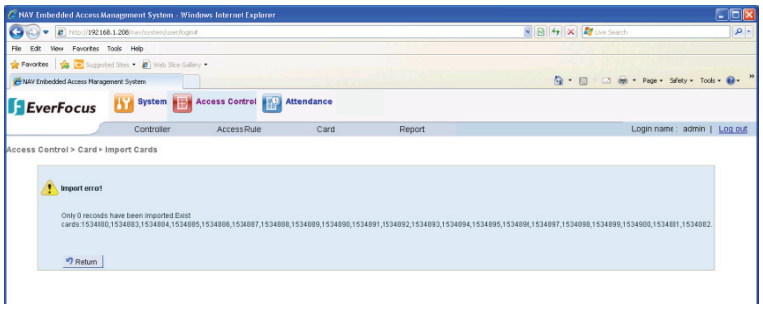


Figure 14-7Card Import Error

4) Click “Back” button, go back the import cards page.

Note: All data imported to the system must be in CVS format, select the path to import the document, click OK to finish.

Chapter 15

15.Report

This chapter describes how to query, print the cards, and access events.

15.1 CardReport

Click on the menu bar “Access Control” → “Report” → “Card Report” and enter to the card report page. Shown as follow:

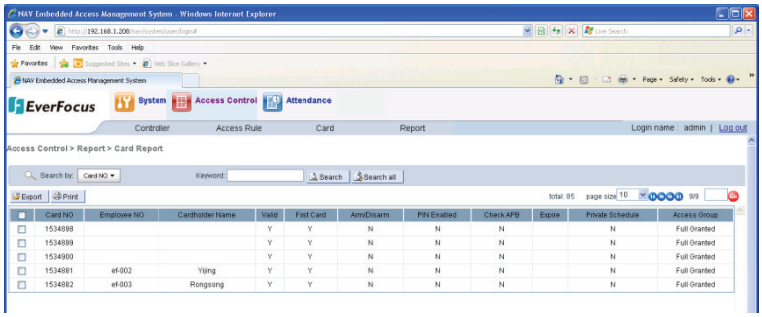


Figure15-1 Card Report

15.1.1 Search Cards

Steps:

1) In the search drop-down menu, select a field, including card number, employee number, and cardholder name, access group.
2) Input the search criteria in the “keyword” text box.
3) Click the “Search” button, the matching cards will be shown in card list.
4) If the user wants to view all the cards in the controller, click the “Search All” button.

15.1.2 Export Cards

Click the “Export” button, pop-up download file box, all cards will be exported to CSV format, select a path to save the file. Click “OK” to confirm. Please see 7.1.7 Export function.

15.1.3 Print Cards

Click the “Print” button to enter to the printing page, the specific operation method see 7.1.8 Print function.

15.2 Card-dependent Event

Click on the menu bar “Access” → “Report” → “Card-dependent Event”, enter to the card-dependent event home page, shown as following:

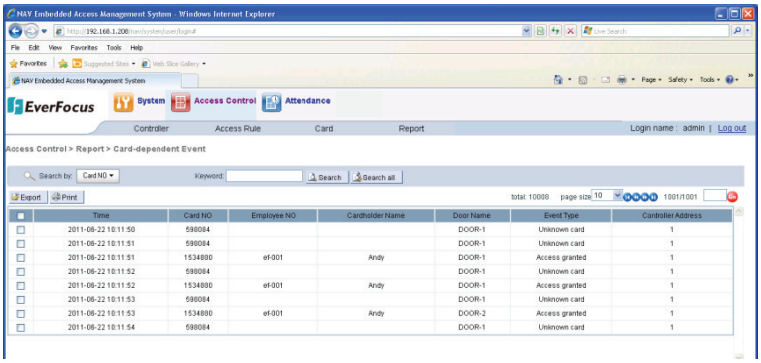


Figure15-2Card-dependent Event

15.2.1 Search Events

Steps:

1) In the search drop-down menu, select a field, including card number, employee number, and cardholder name, event type.
2) Input the search criteria in the “keyword” text box.
3) Click the “Search” button, the matching cards will be shown in card list.
4) If the user wants to view all the cards in the controller, click the “Search All” button.

15.2.2 Export Events

Click the “Export” button, pop-up download file box, all cards will be exported to CSV format, select a path to save the file. Click “OK” to confirm. Please see 7.1.7 Export function.

15.2.3 Print Events

Click the “Print” button to enter to the printing page, the specific operation method see 7.1.8 Print function.

15.3 Card-independent Event

Click on “Access Control” → “Report” → “Card-independent Event” to enter to the card-independent event page.

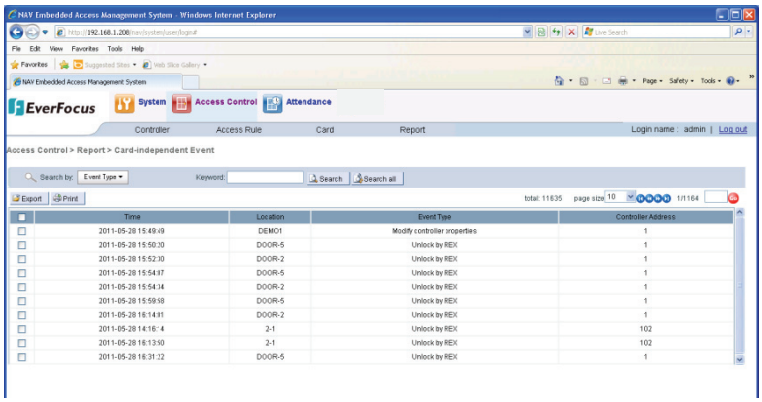


Figure15-3 Card-independentEvent

15.3.1 Search Events

Steps:

1) Select the field “event type”.
2) Input the search criteria in the “keyword” text box.
3) Click the “Search” button, the matching cards will be shown in card list.
4) If the user wants to view all the cards in the controller, click the “Search All” button.

15.3.2 Export Events

Click the “Export” button, pop-up download file box, all cards will be exported to CSV format, select a path to save the file. Click “OK” to confirm. Please see 7.1.7 Export function.

15.3.3 Print Events

Click the “Print” button to enter to the printing page, the specific operation method see 7.1.8 Print function.

Chapter 16

16.Attendance Basic Setting

There are two holiday setting in the software: the first one is to set workdays and weekend during each week for every department (week holiday), and the second one is to set special holidays for every department (special holiday). The second one (special holiday setting) has higher priority than the first one (week holiday setting).For example, if Thursday, April 2nd is set as a workday in the first one and a holiday in the second one, it is treated as a holiday.

Holiday setting priority: group> department > company. The holiday setting in the company is the overall setting. If the setting is different for a department, the department setting is used for attendance management.

In the above figure, the company set Monday to Friday as workdays, Saturday and Sunday as weekend. Three departments: Research and Development, Production Group A and Production Group B set Saturday as a workday. Based on the rule “department > company”, for Research and Development, Production Group A and Production Group B, Monday to Saturday are workdays. All other departments follow the company’s setting in which Monday to Friday are workdays.

16.1 Attendance Time

Click on “Attendance” → “Basic Setting” → “Attendance Time”, and enter to the attendance time setting, shown as following:

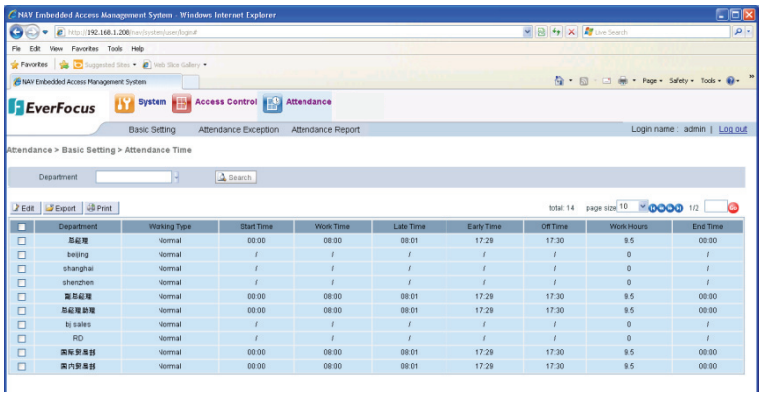


Figure16-1 Attendance Time

The list will be showing the attendance time setting for all departments. In the department drop-down list, select a department. Click the “Search” button to view the department’s setting.

There is no any default setting in the system, just mark by “/” in the list. The user must set the correct attendance time if wants to get the attendance report.

16.1.1 Edit Attendance Time

First time set or reset a department's attendance time.

Select a record to be set in the list, click the "Edit" button to enter to the detail setting page. After set up the attendance time, click the "Save" button to save. Click the "Return" button to back to the list, and the operation is successful.

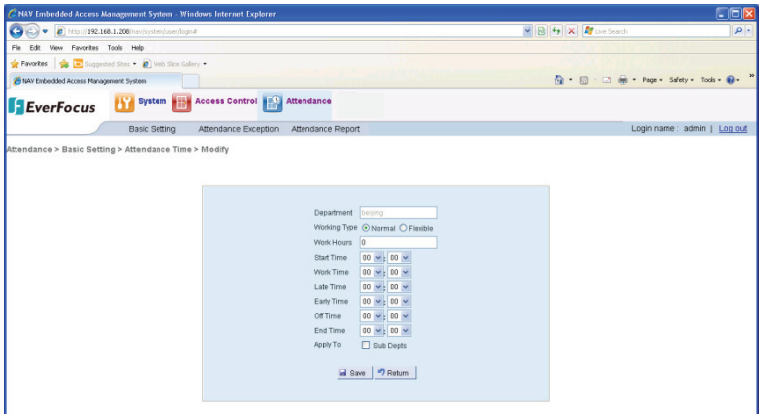


Figure16-2Edit a Department's Attendance Time

16.1.2 Search Attendance Time

Select a department in the drop-down list, and click the "search" button to show the department's attendance time setting, shown as following.

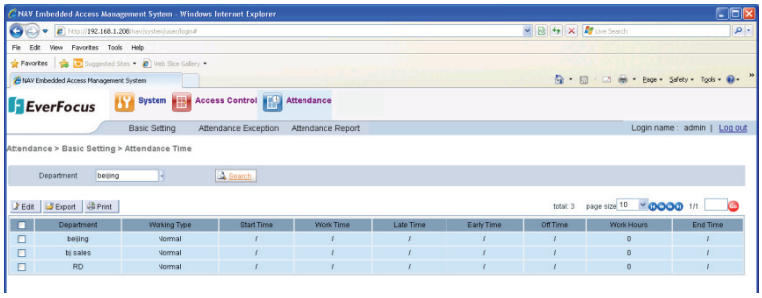


Figure16-3Search a Department's Attendance Time

16.1.3 Export Attendance Time

Click the "Export" button, pop-up download file box, all cards will be exported to CSV format, select a path to save the file. Click "OK" to confirm. Please see 7.1.7 Export function.

16.1.4 PrintAttendance Time

Click the "Print" button to enter to the printing page, the specific operation method see 7.1.8 Print function.

16.2 Week Holiday Setting

Click “Attendance” → “Basic Setting” → “Week Holiday Setting”, enter to the week holiday setting page, shown as following:

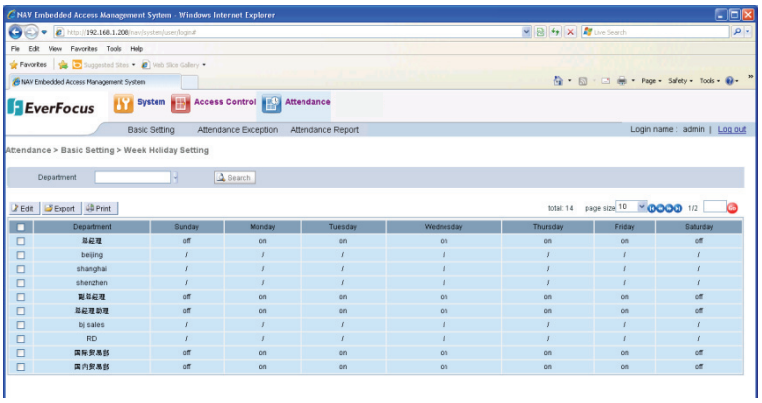


Figure16-4WeekHoliday Setting

The list will be showing the week holiday setting for all departments. In the department drop-down list, select a department. Click the “Search” button to view the department’s setting.

There is no any default setting in the system, just mark by “/” in the list. The user must set the correct week holiday setting if wants to get the attendance report.

16.2.1 Edit AWeek Holiday

First time set or reset a department’s week holiday.

Select a record to be set in the list, click the “Edit” button to enter to the detail setting page. After set up, click the “Save” button to save. Click the “Return” button to back to the list, and the operation is successful.

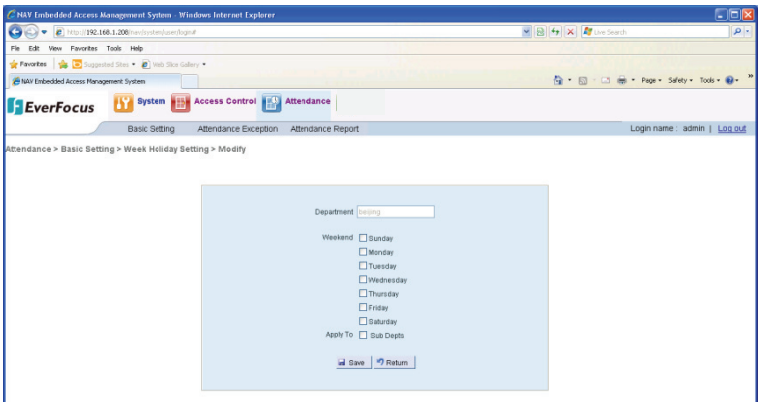


Figure16-5Edit a WeekHoliday

16.2.2 SearchWeek Holidays

Select a department in the drop-down list, and click the “search” button to show the department’s week holiday setting, shown as following.

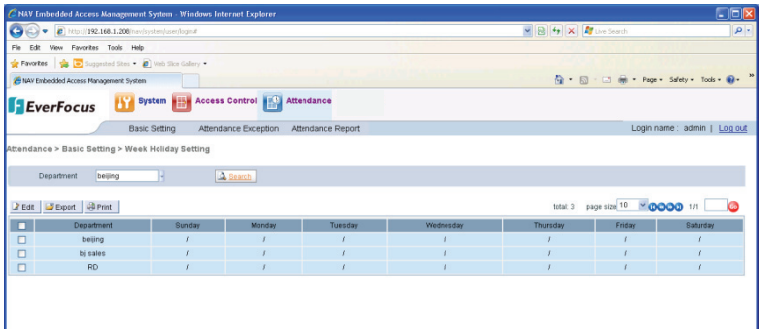


Figure 16-6Search Week Holidays

16.2.3 Export Week Holidays

Click the “Export” button, pop-up download file box, all cards will be exported to CSV format, select a path to save the file. Click “OK” to confirm. Please see 7.1.7 Export function.

16.2.4 Print Week Holidays

Click the “Print” button to enter to the printing page, the specific operation method see 7.1.8 Print function.

16.3 Special Holiday Setting

Click on “Attendance” → “Basic Setting” → “Special Holiday Setting”, and enter to the special holiday setting, shown as following:

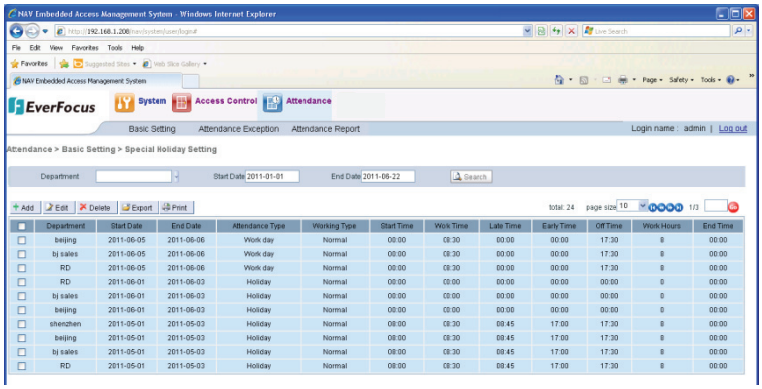


Figure16-7Special Holiday Setting

16.3.1 Add A SpecialHoliday

Click the “Add” button, after adding the special holiday, click the “Save” button to save. Click the “Return” button to back to the list, and the operation is successful.

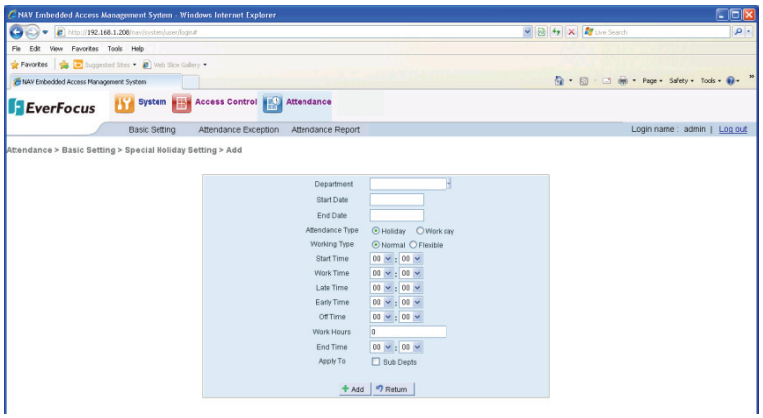


Figure16-8Add a Special Holiday

16.3.2 EditA SpecialHoliday

Select a record to be set in the list, click the “Edit” button to enter to the detail setting page. After modify the special holiday, click the “Save” button to save. Click the “Return” button to back to the list, and the operation is successful.

16.3.3 RemoveA SpecialHoliday

Select a special holiday to be removed in the list. Click the “delete” button, and click “OK” to confirm. The system returns “delete successfully” prompt message indicating that the deleted successfully.

16.3.4 SearchSpecialHolidays

Select a department in the drop-down list, then select a start and end date, and click the “search” button to show the department’s special holiday setting, shown as following.

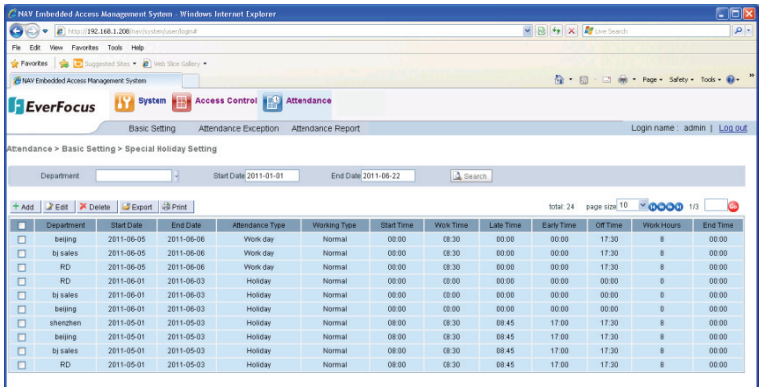

NAV Embedded Access Management System - Windows Internet Explorer
EverFocus
System
Access Control
Attendance
Basic Setting
Attendance Exception
Attendance Report
Login name : admin | Log out
Attendance > Basic Setting > Special Holiday Setting
Department
Start Date 2011-01-01
End Date 2011-06-22
Search
Add
Edit
Delete
Export
Print
total: 24
page size 10
1/3
Department
Start Date
End Date
Attendance Type
Working Type
Start Time
Work Time
Late Time
Early Time
Off Time
Work Hours
End Time
beijing 2011-06-05 2011-06-06 Work day Normal 00:00 08:30 00:00 00:00 17:30 8 00:00
bj sales 2011-06-05 2011-06-06 Work day Normal 00:00 08:30 00:00 00:00 17:30 8 00:00
RD 2011-06-05 2011-06-06 Work day Normal 00:00 08:30 00:00 00:00 17:30 8 00:00
RD 2011-06-01 2011-06-03 Holiday Normal 00:00 00:00 00:00 00:00 00:00 0 00:00
bj sales 2011-06-01 2011-06-03 Holiday Normal 00:00 00:00 00:00 00:00 00:00 0 00:00
beijing 2011-06-01 2011-06-03 Holiday Normal 00:00 00:00 00:00 00:00 00:00 0 00:00
shenzhen 2011-05-01 2011-05-03 Holiday Normal 08:00 08:30 08:45 17:00 17:30 8 00:00
beijing 2011-05-01 2011-05-03 Holiday Normal 08:00 08:30 08:45 17:00 17:30 8 00:00
bj sales 2011-05-01 2011-05-03 Holiday Normal 08:00 08:30 08:45 17:00 17:30 8 00:00
RD 2011-05-01 2011-05-03 Holiday Normal 08:00 08:30 08:45 17:00 17:30 8 00:00

Figure16-9Search Special Days

16.3.5 ExportSpecialHolidays

Click the “Export” button, pop-up download file box, all cards will be exported to CSV format, select a path to save the file. Click “OK” to confirm. Please see 7.1.7 Export function.

16.3.6 PrintSpecialHolidays

Click the “Print” button to enter to the printing page, the specific operation method see 7.1.8 Print function.

Chapter 17

17. Attendance Exception

17.1 No-Access-Attendance

If a staff member forgets to bring or swipe their card, a “no-access-attendance” should be recorded to reflect their actual attendance.

Click on menu options: Attendance →Attendance Exception→No-Access-Attendance, to enter the no-access-attendance page shown on Figure 17-1:

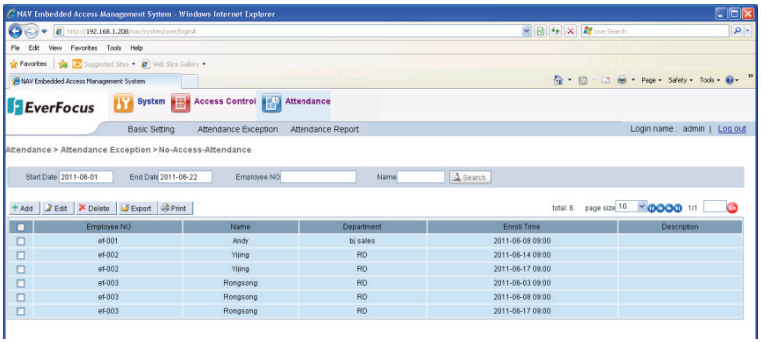


Figure 17-1 No-Access-Attendance Enrollment

17.1.1 AddA No-Access-Attendance

Click the “Add” button to enter the “no-access-attendance enrollment” detail page. Select a record on the list and set employee number, employee name, enrollment date, time and description. Click the “Save” button to apply those settings. Click the “Back” button to return to the list shown on Figure 17-2:

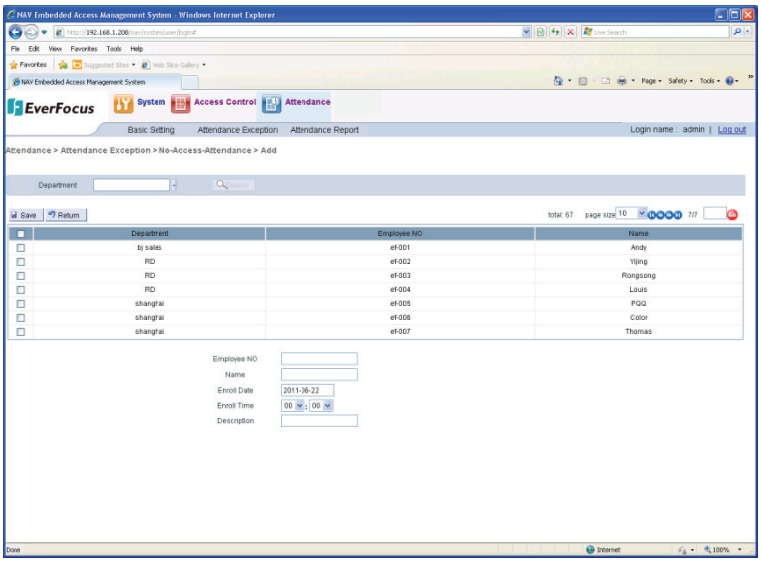


Figure17-2Add a No-Access-Attendance Enrollment

If it is not inconvenient to search through the staff list, you can manually input the employee number or name of the staff member in the “Add No-Access-Attendance” section. The system will automatically apply the additional information needed.

17.1.2 EditA No-Access-Attendance

Select a record that needs editing and click the “Edit” button.

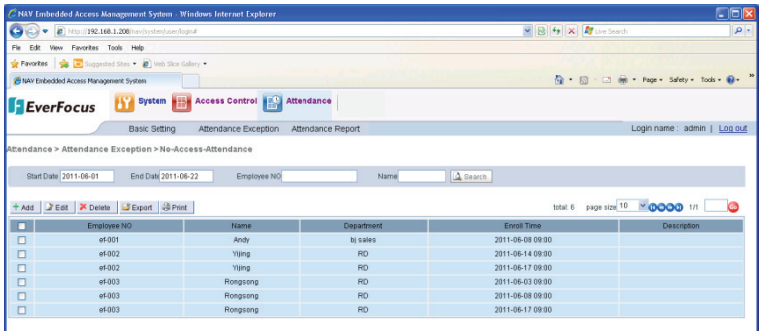


Figure17-3 Edit a No-Access-Attendance Enrollment

Example: Reset a staff member’s enrollment information, such as enroll time. Once the time change is confirmed, click the “Save” button and the system will prompt “Edit successful”. Then click the “return” button to go back to the list, were you can see the enroll time has been modified.

17.1.3 DeleteA No-Access-Attendance

If there is an invalid No-Access-Attendance record, users can delete it.
Select a no-access-attendance record to be deleted and click the “Delete” button. A prompt dialog box will appear asking to ensure the deletion request. To proceed, click the “ok” button and the system will display a confirmation of the deletion request being successful.

17.1.4 SearchNo-Access-Attendance

Users can search No-Access-Attendance.
The system will go to No-Access-Attendance of the present month. Users can search by applying date range, employee ID and staff member name. Click “search” button and if there are no-access-attendance enrollments matching, they will be displayed in the list as shown on Figure17-4:

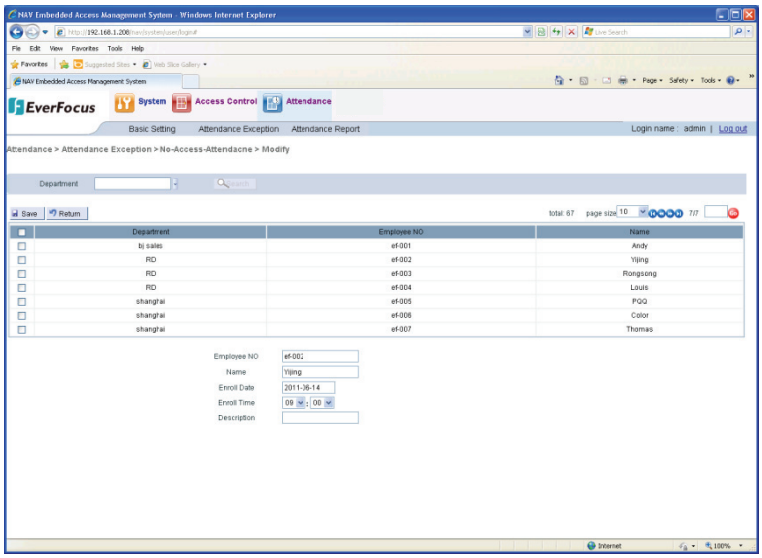


Figure17-4Search No-Access-Attendance Enrollments

17.1.5 ExportNo-Access-Attendance

Click “export” button to transfer all No-Access-Attendance records in a CSV format. A dialog box will appear so a path for a document can be given. Choose a location for the file and click “Ok”. Detailed operational procedures are in section 7.1.7, Export Function.

17.1.6 PrintNo-Access-Attendance

Click the “Print” button to enter a print request of the No-Access-Attendance records. Detailed operation procedures are in section7.1.8, Print Function.

17.2 Time-off Enroll

Function: If a staff member asks for a leave of absence, it is necessary to add a “Time-off Enroll” record to ensure statistical validity of work attendance.

Click the following menu options to enter the page as shown on Figure17-5: Attendance > Attendance Exception > Time-off Enroll.

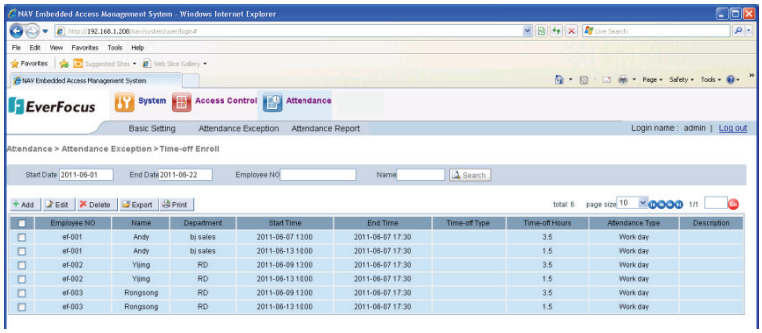


Figure17-5 Time-off Enroll

17.2.1 AddTime-off Enroll

Click the “Add” button to enter the time-off enroll detail page. Select a record on the list, and set the employee number, employee name, start time, end time, time-off type, time-off hours and description. Click the “Save” button after the required information has been filled. Click the “Back” button to return to the list, shown on Figure 17-6:

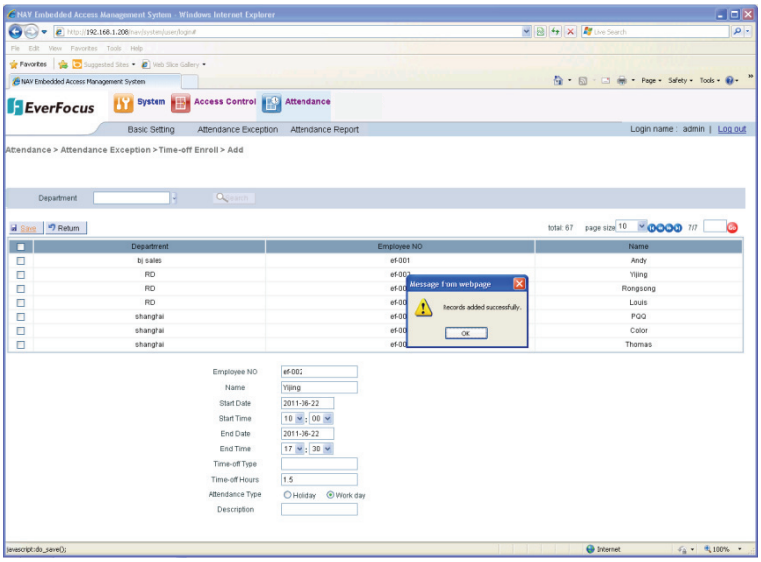


Figure17-6Add Time-off Enroll

If it is not inconvenient to search through the staff list, you can manually input the employee number or name of the staff member in the “Add Time-off Enroll” section. The system will automatically apply the additional information needed

17.2.2 EditTime-off Enroll

Users can edit Time-off Enroll records.

Choose a record in the list of “Time-off Enroll” and click “edit” button as shown on Figure17-7:

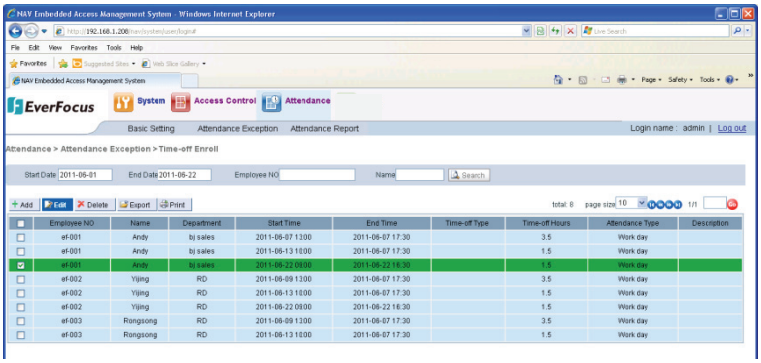


Figure17-7 Selecta Time-off Enrollment

Edit the time-off enrollment’s detail information, as shown on Figure17-8:

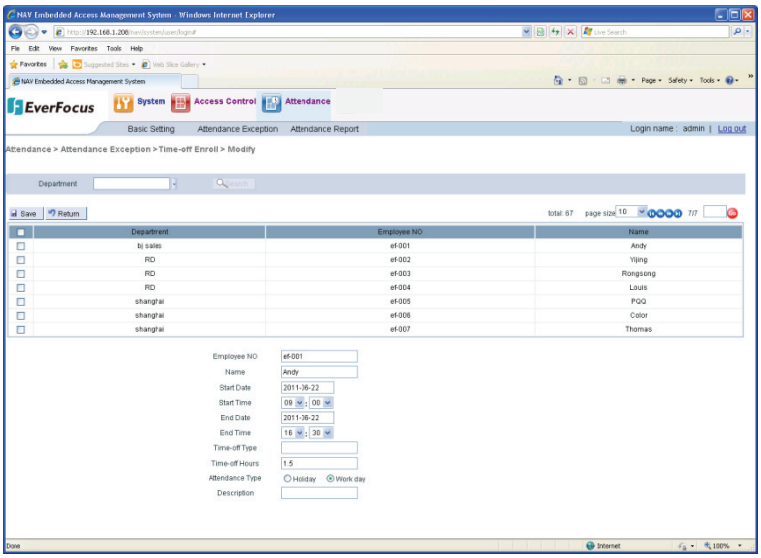


Figure17-8Edit a Time-off Enrollment

Once the change is confirmed, click the “Save” button and the system will prompt “Edit successful”. Then click the “return” button to go back to the list, were you can see the enroll time has been modified.

17.2.3 DeleteTime-off Enroll

If there is an invalid Time-off Enroll record, users can delete it.
Select a Time-off Enroll record to be deleted and click the “Delete” button. A prompt dialog box will appear asking to ensure the deletion request. To proceed, click the “ok” button and the system will display a confirmation of the deletion request being successful.

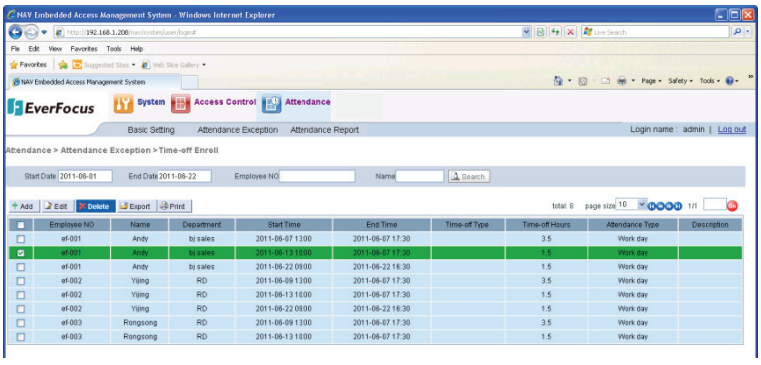


Figure17-9Delete Confirmation of Time-off Enrollment

17.2.4 Search Time-off Enroll

Users can search Time-off Enroll.
The system will go to Time-off Enroll of the present month. Users can search by applying a date range, employee ID and staff member name. Click “search” button and if there are Time-off enrollments matching, they will be displayed in the list.

17.2.5 ExportTime-off Enroll

Click “export” button to transfer all Time-off Enroll records in a CSV format. A dialog box will appear so a path for a document can be given. Choose a location for the file and click “Ok”. Detailed operational procedures are in section7.1.7, Export Function.

17.2.6 PrintTime-off Enroll

Click the “Print” button to enter a print request of the Time-off Enroll records. Detailed operation procedures are in section 7.1.8, Print Function.

17.3 Overtime Enroll

Function: If a staff member works overtime, it is necessary to add “Overtime Enroll” to ensure statistical validity of work attendance.
Click the following menu options to enter the page as shown on Figure17-10: Attendance > Attendance Exception > Overtime Enroll.

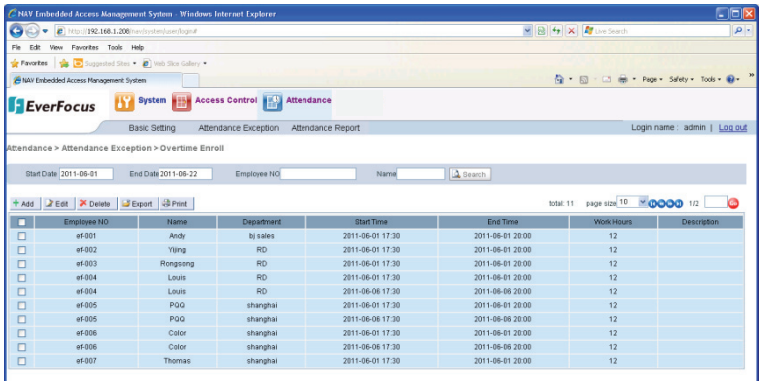


Figure17-10Overtime Enroll

17.3.1 Add Overtime Enroll

Click the “Add” button to enter the Overtime enroll detail page. Select a record on the list, and set the employee number, employee name, start time, end time, time-off type, time-off hours and description. Click the “Save” button after the required information has been filled. Click the “Back” button to return to the list, shown on Figure 17-11:

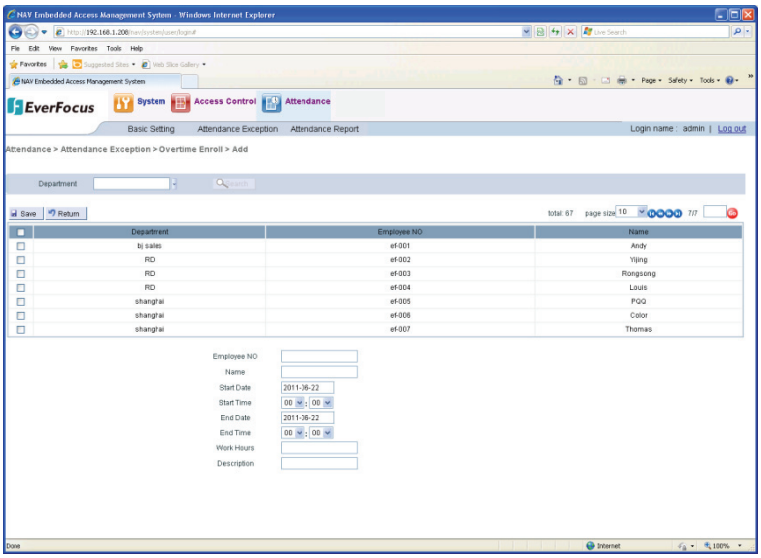


Figure17-3

Add Overtime Enroll

If it is not inconvenient to search through the staff list, you can manually input the employee number or name of the staff member in the “Add Overtime Enroll” section. The system will automatically apply the additional information needed.

17.3.2 Edit Overtime Enroll

Users can edit Overtime Enroll records.

Choose a record in the “Overtime Enroll” list and click “edit” button as shown on Figure 17-12:

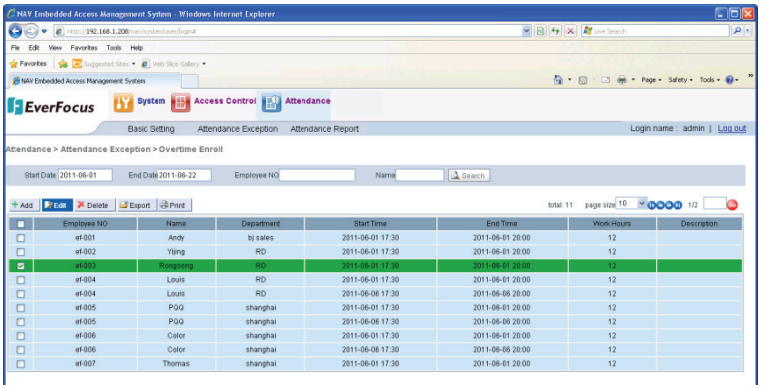


Figure17-4Selecta Overtime Enrollment

Edit the Overtime enrollment’s detail information, as shown on Figure 17-13:

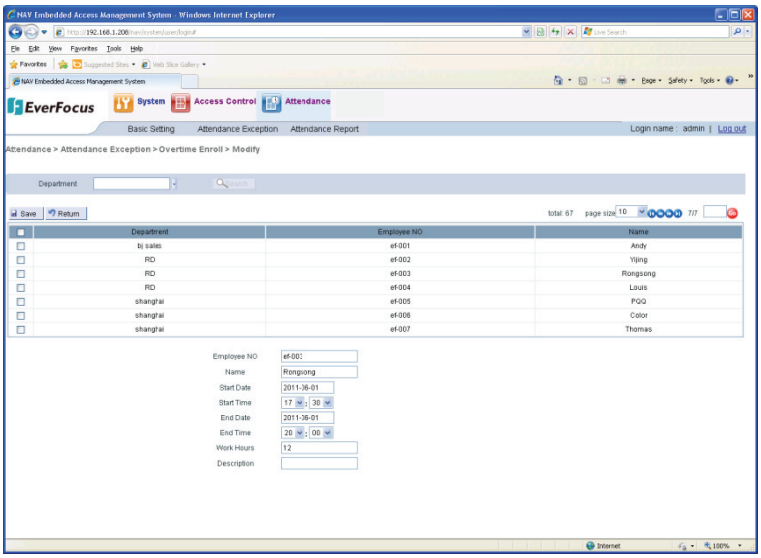


Figure17-5Edit a Overtime Enrollment

Once the change is confirmed, click the “Save” button and the system will prompt “Edit successful”. Then click the “return” button to go back to the list, were you can see the overtime record has been modified.

17.3.3 DeleteOvertime Enroll

If there is an invalid Overtime Enroll record, users can delete it.
Select an Overtime Enroll record to be deleted and click the “Delete” button. A prompt dialog box will appear asking to ensure the deletion request. To proceed, click the “ok” button and the system will display a confirmation of the deletion request being successful.

17.3.4 SearchOvertime Enroll

Users can search Overtime Enroll.
The system will go to Overtime Enroll of the present month. Users can search by applying a date range, employee ID and staff member name. Click the “search” button and if there are Overtime enrollments matching, they will be displayed in the list.

17.3.5 ExportOvertime Enroll

Click “export” button to transfer all Overtime Enroll records in a CSV format. A dialog box will appear so a path for a document can be given. Choose a location for the file and click “Ok”. Detailed operational procedures are in section 7.1.7, Export Function.

17.3.6 PrintOvertime Enroll

Click the “Print” button to enter a print request of the Overtime Enroll records. Detailed operation procedures are in section 7.1.8, Print Function.

Chapter 18

18.Attendance Report

18.1 Original Access Record

To review the Original Access Record Section, Click the following menu options to enter the page as shown on Figure 18-1: Attendance > Attendance Report >Original Access Record.

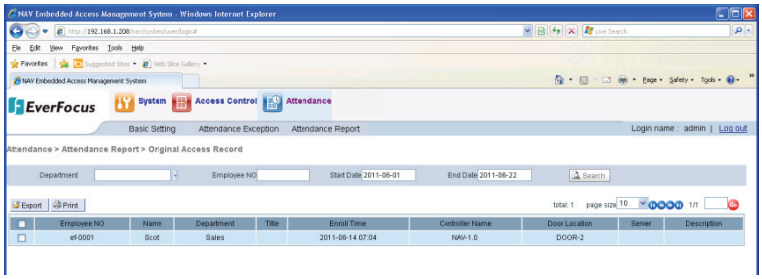


Figure18-1 Original Access Record

18.1.1 Search Original Access Records

If users wish to search an employee original access records, the employee's ID number is required in the "Employee NO" section. If users wish to search all employee records under a specific department, simply select a department in the "Department" drop-down list.

Steps:

1) Choose the department in the "Department" drop down or input the employee's ID number in the "Employee NO" section.
2) Input start date and end date.
3) Click the "Search" button.

The records matching will be shown in the list.

18.1.2 ExportOriginal Access Records

Click "export" button to transfer all Original Access Records in a CSV format. A dialog box will appear so a path for a document can be given. Choose a location for the file and click "Ok". Detailed operational procedures are in section 7.1.7, Export Function.

18.1.3 PrintOriginal Access Records

Click the "Print" button to enter a print request of the Original Access Records. Detailed operation procedures are in section 7.1.8, Print Function.

18.2 Report by Cardholder

To review the Report by Cardholder Section, Click the following menu options to enter the page as shown on Figure 18-2: Attendance →Attendance Report→Report by Cardholder.

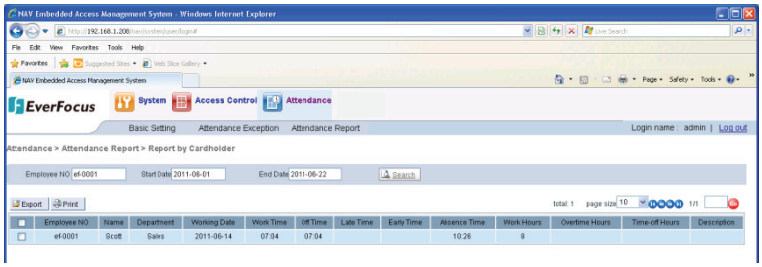


Figure 18-2Report by Cardholder

The Report by Cardholder section reflects employee number, name, department, working date, work time, off time, late time, early time, absence time, work hours, overtime hours, time-off hours and description.

18.2.1 GenerateReport by Cardholder

Steps:

1) Input the employee number in the “Employee NO” box.
2) Input the start and end time.
3) Click the “Search” button

The matching records will be shown in the list.

18.2.2 Export Report by Cardholder

Click “export” button to transfer all Report by Cardholder Records in a CSV format. A dialog box will appear so a path for a document can be given. Choose a location for the file and click “Ok”. Detailed operational procedures are in section 7.1.7, Export Function.

18.2.3 Print Report by Cardholder

Click the “Print” button to enter a print request of the Report by Cardholder records. Detailed operation procedures are in section 7.1.8, Print Function.

18.3 Statistics by Cardholder

To review the Statistics by Cardholder Section, Click the following menu options to enter the page as shown on Figure 18-3: Attendance > Attendance Report>Statistics by Cardholder.

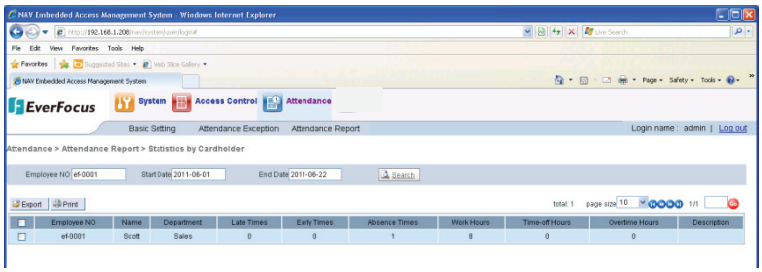


Figure18-3 Statistics by Cardholder

18.3.1 GenerateStatistics by Cardholder Report

Steps:

1) Input the employee number in the “Employee NO” box.
2) Input the start and end time.
3) Click the “Search” button, the matching records will be shown in the list.

18.3.2 Export Statistics by Cardholder Report

Click “export” button to transfer all Statistics by Cardholder Records in a CSV format. A dialog box will appear so a path for a document can be given. Choose a location for the file and click “Ok”. Detailed operational procedures are in section 7.1.7, Export Function.

18.3.3 Print Statistics by Cardholder Report

Click the “Print” button to enter a print request of the Statistics by Cardholder records. Detailed operation procedures are in section 7.1.8, Print Function.

18.4 Statistics By Department

To review the Statistics by Department Section, Click the following menu options to enter the page as shown on Figure 18-4:Attendance > Attendance Report>Statistics by Department.

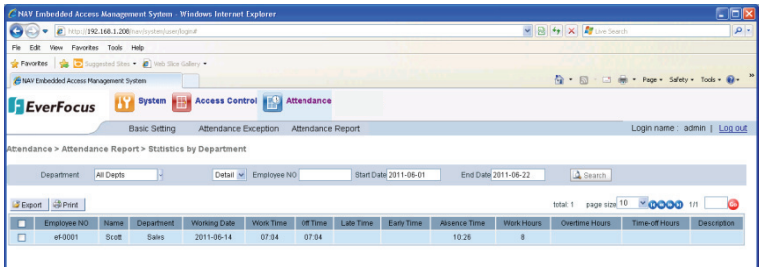


Figure 18-4 Report by a Department

The report can be generated in two ways: Report by Department and Statistics by Department.

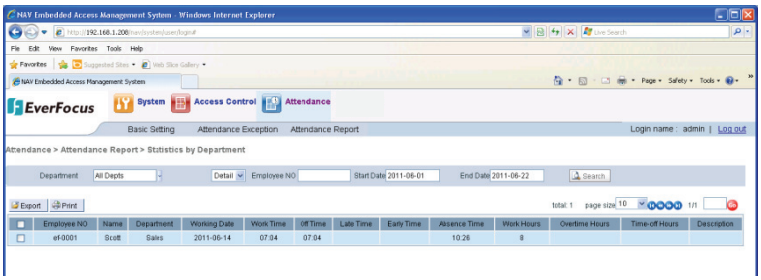


Figure 18-5 Statistics by a Department

18.4.1 Generate Statistics by Department Report

Steps:

1) Select a department in the department box.
2) Select the method to generate the report.
3) Input start and end time.
4) Click the “Search” button, the matching records will be shown in the list.

18.4.2 Export Statistics by Department Report

Click “export” button to transfer all Statistics by Department Records in a CSV format. A dialog box will appear so a path for a document can be given. Choose a location for the file and click “Ok”. Detailed operational procedures are in section 7.1.7, Export Function.

18.4.3 Print Statistics by Department Report

Click the “Print” button to enter a print request of the Statistics by Department records. Detailed operation procedures are in section 7.1.8, Print Function.

EverFocus Electronics Corp.

Head Office
12F, No.79 Sec.1 Shin-Tai Wu Road,
Hsi-Chi, Taipei, Taiwan
Tel : + 886-2-2698-2334
Fax : + 886-2-2698-2380

European Office
Albert-Einstein-Strasse 1,
D-46446 Emmerich, German
Tel : + 49-2822-9394-0
Fax : + 49-2822-939495

USA Office
1801 Highland Ave, Duarte,
Building
CA 91010 ,U.S.A
Tel : + 1-626-844-8888
Fax : + 1-626-844-8838

Beijing Office
Room 609, KEMAO Building,
Shangdi, Haidian, Beijing, China
Tel : + 86-10-6297-3336
Fax : + 86-10-6297-1423

Japan Office
1809 WBG Marive East 18F,
2-6 Nakase, Mihama-ku,
Chiba city 261-7118, Japan
Tel : + 81-43-212-8188
Fax : + 81-43-297-0081

Shenzhen Office
4F, No.2, D4 Building, Wanyelong
Industrial Park, Tangtou Road,
Shiyan, Baoan, Shenzhen,
Guangdong, China
Tel: +86-755- 27651313
Fax: +86-755-27650337

EverFocus
4605PNC302X020A
V 2.0